Transport and Communications Science Journal, Vol 76, Issue 03 (04/2025), 271-281

Transport and Communications Science Journal

APPLICATION OF GROVER'S QUANTUM SEARCH ALGORITHM ATTACK ON S-DES CRYPTOGRAPHY

Tat Thang Nguyen[1], Thanh Toan Dao[1,*], Nhu Quynh Luc[2,*]

[1]University of Transport and Communications, 3 Cau Giay, LangHa, Dong Da, Hanoi, Vietnam

[2]Academy of Cryptography Techniques, 141 Chien Thang, TanTrieu, ThanhTri, Hanoi, Vietnam

ARTICLE INFO

TYPE: Research Article
Received: 19/01/2025
Revised: 04/04/2025
Accepted: 10/04/2025
Published online: 15/04/2025
https://doi.org/10.47869/tcsj.76.3.6

[*] *Corresponding author*
Email: quynhln@actvn.edu.vn, daotoan@utc.edu.vn

Abstract. With the advent of quantum computers, many cryptographic systems in use today can be broken with fast execution speed. Cryptanalysis algorithms using quantum computing are still modest and are in the research stage. For block cipher systems, the quantum Grover search algorithm is a popular tool. Grover's algorithm has the advantage of using amplitude amplification techniques to speed up and reduce time significantly, reducing the computational complexity of the algorithm. Specifically, Grover's algorithm is a quantum algorithm used to search an unsorted database of N elements, in which the time complexity is $O(\sqrt{N})$ and uses $O(\log N)$ storage space. In Mishal Almazrooie's work, he proposed a method to prove and demonstrate the feasibility of applying Grover's search algorithm to cryptanalysis of the S-DES symmetric key cryptosystem. Based on international and domestic research, in this study, the authors implement the S-DES cryptosystem using Grover's algorithm with the aim of testing the feasibility and orienting the application of this algorithm to explore other block cipher systems in future publications.

Keywords: Grover algorithm, Qiskit, S-DES, Quantum CNOT gate, Quantum Hadamard gate.

Tạp chí Khoa học Giao thông vận tải

ỨNG DỤNG THUẬT TOÁN TÌM KIẾM GROVER LƯỢNG TỬ TRONG TẤN CÔNG HỆ MẬT S-DES

Nguyễn Tất Thắng[1], Đào Thanh Toản[1,*], Lục Như Quỳnh[2,*]

[1]Trường Đại học Giao thông vận tải, Số 3 Cầu Giấy, Láng Hạ, Đống Đa, Hà Nội, Việt Nam

[2]Học viện Kỹ thuật mật mã, Số 141 Chiến Thắng, Tân Triều, Thanh Trì, Hà Nội, Việt Nam

THÔNG TIN BÀI BÁO

CHUYÊN MỤC: Công trình khoa học
Ngày nhận bài: 19/01/2025
Ngày nhận bài sửa: 04/04/2025
Ngày chấp nhận đăng: 10/04/2025
Ngày xuất bản Online: 15/04/2025
https://doi.org/10.47869/tcsj.76.3.6

** Tác giả liên hệ*
Email: quynhln@actvn.edu.vn, daotoan@utc.edu.vn

Tóm tắt. Với sự xuất hiện của máy tính lượng tử, nhiều hệ mật đang sử dụng hiện nay có thể bị phá vỡ với tốc độ thực thi nhanh. Các thuật toán thám mã sử dụng tính toán lượng tử còn khiêm tốn và đang trong giai đoạn nghiên cứu. Đối với các hệ mã khối, thuật toán tìm kiếm Grover lượng tử được áp dụng là công cụ phổ biến. Thuật toán Grover có ưu điểm đến pha tính toán lượng tử sử dụng kỹ thuật khuếch đại biên độ với mục đích tăng tốc và giảm thời gian đáng kể, giảm độ phức tạp tính toán của thuật toán. Cụ thể, thuật toán Grover là một thuật toán lượng tử dùng trong việc tìm kiếm một cơ sở dữ liệu chưa sắp xếp N phần tử, trong đó độ phức tạp về thời gian là $O(\sqrt{N})$ và sử dụng $O(\log N)$ không gian lưu trữ. Trong công trình của Mishal Almazrooie đã đưa ra phương pháp chứng minh và tính khả thi áp dụng thuật toán tìm kiếm Grover vào thám hệ mật mã khóa đối xứng S-DES. Dựa trên các nghiên cứu trên thế giới và trong nước, trong nghiên cứu này, các tác giả thực thi thám hệ mật S-DES sử dụng thuật toán Grover với mục tiêu kiểm nghiệm tính khả thi và định hướng áp dụng thuật toán này để thám với các hệ khác về mã khối trong các công bố tiếp theo.

Từ khóa: Thuật toán Grover, Qiskit, hệ mật đơn giản DES (S-DES), Cổng C-NOT lượng tử, Cổng Hadamard lượng tử.

1. GIỚI THIỆU

Tính toán lượng tử đã được các nhà khoa học nghiên cứu và đã có nhiều công bố từ những

năm 1982 gồm có Deutsch, Deutsch-Jozsa, Simon, Peter Shor, Grover,… các thuật toán này có thể được ứng dụng trong mật mã gồm: (1) Các thuật toán Deutsch [1], Deutsch-Jozsa [2], Simon [3], Grover được ứng dụng trong thám mã của hệ mật khóa đối xứng [4]; (2) Thuật toán Peter Shor được ứng dụng trong thám mã với hệ mật khóa công khai. Hiện nay, đối với các thuật toán tính toán lượng tử (Deutsch, Deutsch-Jozsa, Simon, Grover) ứng dụng trong mật mã khóa đối xứng đã có các nghiên cứu và phát triển như Quantum Walk, biến đổi Fourier lượng tử [5], khuếch đại biên độ,… điển hình của kỹ thuật khuếch đại biên độ là thuật toán Grover [6],[7].

Năm 1996, thuật toán tìm kiếm Grover lượng tử được đề xuất bởi Lov Grover. Mục tiêu của thuật toán là giải bài toán "tìm kiếm một chuỗi trong tập cơ sở dữ liệu chưa xắp xếp gồm N phần tử", với độ phức tạp tính toán là O($\sqrt{N}$) và sử dụng O(log N) không gian lưu trữ. Trong máy tính lượng tử, nếu một hàm $y = f(x)$ là cân bằng, thuật toán Grover cho phép tính được giá trị x khi đã biết y với số lượng phép truy vấn ít hơn (tức là giải được bài toán tìm ánh xạ nghịch đảo). Điều này, cho thấy tính hiệu quả của thuật toán tìm kiếm Grover trong tìm kiếm một chuỗi bit. Khi đó, với kịch bản "biết trước một số lượng nhất định cặp bản rõ-mã của hệ mật mã khóa đối xứng", khi đó có thể tìm kiếm khóa sử dụng thuật toán tìm kiếm Grover lượng tử (ở đây sử dụng thuật toán Grover với trường hợp k biết trước).

Simplified-Data Encryption Standard (S-DES) là phiên bản đơn giản của hệ mật DES nổi tiếng do Schaefer phát triển [8]. Với các tham số nhỏ, S-DES có các đặc tính và cấu trúc tương tự như DES [9]. Cấu trúc nhỏ của S-DES thể hiện chính xác cấu trúc của DES gốc. Do đó, S-DES là một nghiên cứu điển hình để ứng dụng thuật toán Grover trong việc thám mã. Công bố [10], [11] đã đưa ra thiết kế mạch lượng tử và ước tính tài nguyên lượng tử cho việc tìm kiếm khóa bằng thuật toán Grover khi hệ mật mã khối S-DES hoạt động.

Trong nghiên cứu này, với mục tiêu nghiên cứu và phân tích khả năng tấn công vào các hệ mật mã khối hiện nay bằng công cụ tính toán lượng tử, các tác giả đã thực hiện khảo sát, phân tích lý thuyết về ưu nhược điểm của thuật toán tìm kiếm Grover. Áp dụng thuật toán Grover trong thám mã với hệ mật mã khối S-DES. Đây chính là cơ sở giúp nhóm có các tiền đề để nghiên cứu áp dụng thuật toán tìm kiếm Grover trong việc thám mã với các hệ mật mã khối khác như DES, AES trong tương lai. Các khảo sát và phân tích về thuật toán Grover lượng tử được các tác giả trình bày cụ thể trong các thảo luận phía sau của công bố.

2. THUẬT TOÁN LƯỢNG TỬ TÌM KIẾM GROVER

2.1. Thuật toán lượng tử tìm kiếm Grover

Theo công bố [11], thuật toán tìm kiếm Grover được triển khai theo 4 giai đoạn: Khởi tạo, oracle, khuếch đại biên độ và đo lường.

Thuật toán 1: Tìm kiếm Grover lượng tử

---

1. Khởi tạo vector a với giá trị ban đầu được gán bằng j.

$|\psi_0\rangle = |0\rangle^{\otimes n} \otimes H|1\rangle$

2. Đặt thanh ghi vào một chồng chất phân bố đều

$|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} = H^{\otimes n}.\ |0\rangle^{\otimes n} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$

3. Lặp lại vòng lặp Grover $t_k \approx \frac{n}{2}$ lần theo từng bước như sau:

3.1. Áp dụng Ref_m cho vector a thông qua Grover Oracle U_s, thu được vector a'.

$|\psi_2\rangle = U_s(|\psi_1\rangle)$

3.2. Áp dụng Ref_j cho a', thu được giá trị mới của a. Tính $|\psi_3\rangle$

4. Đo trạng thái cuối cùng của vector a, tính $|\psi_4\rangle$ cho ra một chuỗi $x \in \{0,1\}^n$.

Ý tưởng hoạt động của thuật toán Grover:

Thuật toán này được thực hiện với 4 bước chính (thuật toán 1). Các bước 1, 2 và 4 được thực hiện trên máy tính cổ điển và lượng tử có độ phức tạp tương đương. Tuy nhiên, trong bước 3, với sự góp sức của máy tính lượng tử thì khả năng tính toán được giảm nhiều. Điều này được thể hiện bởi tính ưu việt xử lý tính toán của hàm Oracle (U_S) và hàm Diffusion (Ref_j)

Tính đúng đắn của thuật toán Grover:

Thuật toán Grover được dùng để giải quyết bài toán tìm kiếm vét cạn. Giả sử ta có một không gian kích thước N và có một phần tử đặc biệt. Trong trường hợp xấu nhất sẽ phải kiểm tra tất cả các phần tử, và thậm chí, thuật toán ngẫu nhiên cũng phải kỳ vọng xem xét tới $\frac{N}{2}$ phần tử. Để giải thích cho điều này, ta gọi A là tập hợp gồm N phần tử: $A = \{a_1, a_2, \dots, a_N\}$. Xác xuất để chọn phần tử từ tập A là:

$$P\{a_1\} = P\{a_2\} = \cdots = P\{a_N\} = \frac{1}{N} \quad (1)$$

Từ đó, giá trị kì vọng của số lần lấy phần tử từ tập A cho đến khi ta tìm được phần tử đặc biệt là:

$$E(x) = \sum_{k=1}^{N} k \cdot P(x = k) = \sum_{k=1}^{N} k \frac{1}{N} = \frac{1}{N} \cdot \frac{N \cdot (N+1)}{2} = \frac{N+1}{2} \quad (2)$$

Tốc độ của thuật toán lượng tử Grover là $\frac{N}{2}$ có thể cải thiện tới $O(N^{\frac{1}{2}})$. So với thuật toán tìm kiếm ngẫu nhiên, trị số $\frac{1}{2}$ được đưa lên số mũ, và đây là một sự cải thiện lớn.

Cho k là số nghiệm khác 0. Sau khi chia vector h cho $\sqrt{k}$, h trở thành một vector đơn vị, do đó có trạng thái lượng tử hợp lệ:

$$h(x) = \begin{cases} \frac{1}{\sqrt{k}}, & \text{nếu } x \text{ là nghiệm} \\ 0, & \text{nếu } x \; không \text{ là nghiệm} \end{cases}$$

Định nghĩa vector trượt đích m:

$$m(x) = \begin{cases} 0, & \text{nếu } x \text{ là nghiệm} \\ \frac{1}{\sqrt{N-k}}, & \text{nếu } x \; không \text{ là nghiệm} \end{cases}$$

Từ đó m cũng thuộc vào không gian con, vì:

$$m = \frac{1}{\sqrt{N-k}} \left(\sqrt{N} j - \sqrt{k} h\right), \quad (3)$$

và quan trọng, là nó trực giao với h do:

$$m \cdot h = \left(\frac{1}{\sqrt{N-k}}, \dots, 0, \frac{1}{\sqrt{N-k}}, \dots, \frac{1}{\sqrt{N-k}}, 0, \dots, \frac{1}{\sqrt{N-k}}\right)\left(0, \dots, \frac{1}{\sqrt{k}}, 0, \dots, 0, \frac{1}{\sqrt{k}}, \dots, 0\right) = 0 \quad (4)$$

Do m là vector đặc trưng của tập $\bar{S}$ nên phản xạ của vector a qua m có thể sử dụng Grover oracle $U_{\bar{S}}$. Mà $\bar{\bar{S}} = S$, nên phản xạ của vector a qua m: có thể sử dụng Grover oracle U_S.

Phản xạ qua m sử dụng Grover oracle của tập S, được định nghĩa bởi:

$$U_S[x, y] = \begin{cases} -1 & nếu\ x = y \in S \\ 1 & nếu\ x = y \notin S \\ 0 & nếu\ x \neq y \end{cases}$$

Đặt θ là góc hợp giữa m và a trước những vòng lặp của thuật toán Grover. Giả sử: $\alpha \leq \theta \leq \frac{\pi}{2}$; m đóng vai trò là trục Ox, góc hợp giữa a' và j bây giờ là $\alpha + \theta$. Lúc này, phép phản xạ a' qua j biến a' thành a. Góc hợp giữa a và j lúc này là $2(\alpha + \theta)$. Do đó, góc hợp của vector a với trục Ox sau vòng lặp Grover đầu tiên là:

$$\theta' = -\theta + 2(\alpha + \theta) = \theta + 2\alpha \quad (5)$$

Hàm Oracle $f(x)$ trong thuật toán Grover định nghĩa là:

$$f(x) = \begin{cases} 1 & \text{nếu } x \text{ là nghiệm} \\ 0 & \text{nếu } x\ khôngg \text{ là nghiệm} \end{cases} \quad (6)$$

Hoạt động của hàm Oracle được biểu diễn trong toán học:

$$|x\rangle|q\rangle \rightarrow (-1)^{f(x)}|x\rangle|q\rangle \quad (7)$$

với $|x\rangle$ là trạng thái đầu vào, $f(x)$ trả về 1 nếu x là giải pháp và 0 nếu ngược lại.

Hàm Diffusion làm tăng xác suất tìm kiếm được phần tử đúng, tăng xác suất đo được các trạng thái âm (trạng thái đúng), trong khi giảm xác suất đo được các trạng thái dương. Hàm Diffusion được biểu diễn dưới dạng toán học như sau:

$$\mathcal{D} = H^{\otimes n}(2|j\rangle\langle j| - I)\, H^{\otimes n} \quad (8)$$

Biểu diễn toán học này minh họa các toán tử khuếch đại biến đổi các biên độ của các trạng thái trong trạng thái chồng chất lượng tử, tăng xác suất đo được trạng thái mục tiêu. Đây là một hàm giúp cho việc tăng độ bậc hai của thuật toán.

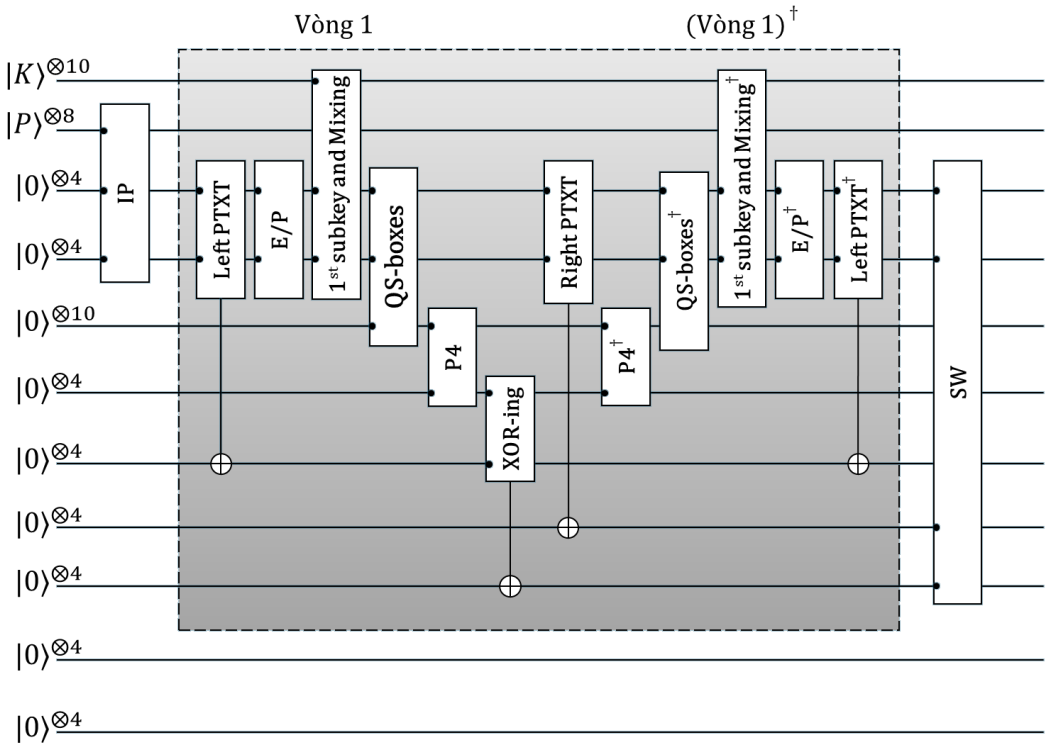
Trong nghiên cứu này, tác giả đã sử dụng với máy tính Intel® Core™ i7-10700 2.90 GHz, RAM: 8 GB DDR4 2400 MHz, SSD: 256 GB, và được kết nối với máy tính lượng tử của IBM. Máy tính lượng tử của IBM có cấu hình chi tiết: 32 Qubit, Max shots = 20000, Max circuits = 300, Max qubits/gate = 3, and Max channels gate = 9, việc kết nối này thông qua hàm API.

IBM đã cung cấp các trình mô phỏng tiên tiến thực hiện các thuật toán lượng tử trên các bộ xử lý thông thường, cạnh các thiết bị phần cứng thực [12]. Với máy tính lượng tử, hiện nay

có nhiều công cụ được hỗ trợ như nền tảng ngôn ngữ lập trình Qiskit ([13]) và thư viện libquantum 0.9.1 ([14]) để thiết kế thử nghiệm ứng dụng chạy trên máy tính lượng tử thực và máy tính lượng tử ảo. Trong đó, với công việc triển khai các ứng dụng thường được các nhà khoa học chọn nền tảng mô phỏng với hỗ trợ trên các máy tính hiện có, chính vì thế thư viện libquantum 0.9.1 là giải pháp tốt được sử dụng hiện nay. Thư viện libquantum 0.9.1 được cài đặt và có nhiều hỗ trợ trên các hệ máy tính với hệ điều hành ubuntu hiện nay. Libquantum 0.9.1 là thư viện C để mô phỏng cơ học lượng tử, tập trung vào tính toán lượng tử [14]. Dựa trên các nguyên tắc của cơ học lượng tử, libquantum cung cấp cách triển khai thanh ghi lượng tử. Các thao tác cơ bản để tương tác với cổng Hadamard lượng tử hoặc cổng Controlled-NOT lượng tử (CNOT) đều có sẵn dễ sử dụng. Các phép đo có thể được thực hiện trên các qubit đơn lẻ hoặc toàn bộ thanh ghi lượng tử.

2.2. Ứng dụng thuật toán lượng tử tìm kiếm Grover

Mạch lượng tử được đề xuất cho thuật toán lượng tử tìm kiếm Grover hệ mật S-DES theo [11] được thể hiện ở Hình 1.



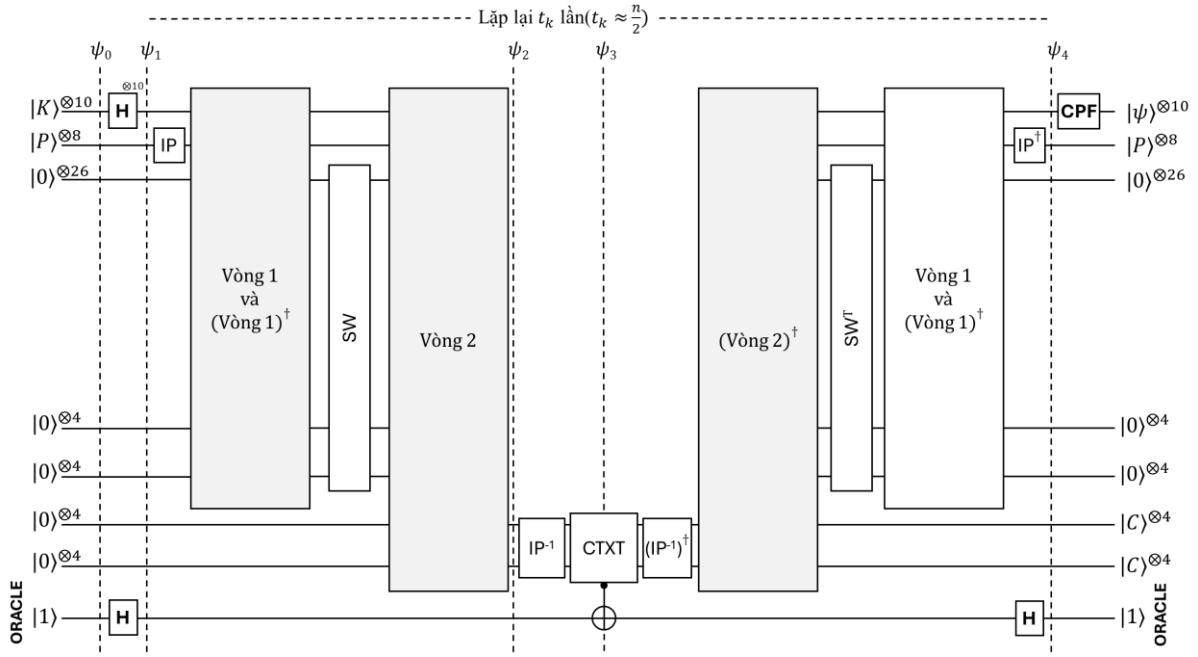
Hình 1. Mạch lượng tử cho hệ mật S-DES [11].

Để người thám mã lượng tử tấn công vào mã khối thì yêu cầu đầu tiên phải có là một mạch đảo lượng tử. Người thám mã lượng tử triển khai một mã khối như một mạch lượng tử hoàn chỉnh có thể đảo ngược, mạch lượng tử có thể được tích hợp như một hàm trong một oracle hoặc hộp đen. Hộp đen là một hàm boolean trong các thuật toán lượng tử. Khi một cuộc tấn công Grover đối với S-DES được thực hiện, bước đầu tiên trong việc triển khai cuộc tấn công là xây dựng Oracle được thể hiện trong phương trình (7). Mạch lượng tử của S-DES được mô hình như một hàm Boolean $f(k)$ để thay thế hàm trong phương trình (6) như sau:

$$f(k) = \begin{cases} 1, & nếu\ SDES(k, p_*) = c_* \\ 0, & nếu\ SDES(k, p_*) \neq c_* \end{cases} \quad (9)$$

$$|k\rangle \overset{U_f}{\rightarrow} (-1)^{f(k)}|k\rangle \tag{10}$$

Trong phương trình (10), $|k\rangle$ là không gian trạng thái của khóa, U_f là Oracle được truy vấn trên $|k\rangle$, và trong hàm Boolean $f(k)$, cặp p_* và c_* là cặp văn bản rõ-mã tương ứng của mã hóa S-DES.



Hình 2. Áp dụng thuật toán Grover cho hệ mật S-DES [11].

Hình 2 minh họa mô hình hoàn chỉnh của cuộc thuật toán Grover tấn công đối với hệ mật S-DES. Tại $|\psi_0\rangle$, các thanh ghi lượng tử được khởi tạo, tất cả các qubit bao gồm cả qubit của Oracle được đặt thành $|0\rangle$, tạo thành trạng thái ban đầu của hệ thống: $|\psi_0\rangle = |0\rangle^{\otimes 16} \otimes |0\rangle$.

3. KẾT QUẢ VÀ THẢO LUẬN

Thực thi thuật toán lượng tử tìm kiếm Grover trong tìm kiếm khóa hệ mật S-DES được mô phỏng trên mã nguồn mở Ubuntu 18.04 sử dụng ngôn ngữ lập trình C. Một số phần mềm và thiết bị sử dụng máy tính có cấu hình CPU: Intel® Core™ i7-10700 2.90 GHz, RAM: 8 GB DDR4 2400 MHz, SSD: 256 GB. Trong đó, có tích hợp thư viện libquantum 0.9.1 trong hệ điều hành Ubuntu 18.04.

Thuật toán lượng tử Grover tìm kiếm trong một cơ sở dữ liệu chưa được sắp xếp được thực hiện theo các bước [11]:

Bước 1: Khởi tạo thanh ghi lượng tử

Bước 2: Đặt các thanh ghi vào trạng thái chồng chất lượng tử bằng cách sử dụng tập hợp các cổng Hadamard H. Đưa qubit của Oracle vào trạng thái $|1\rangle$ bằng cách áp dụng một cổng Pauli-X sau đó chuyển sang trạng thái chồng chất nhờ cổng Hadamard H.

Bước 3: Áp dụng hàm Oracle. Hàm Oracle được cài đặt để đánh dấu trạng thái mục tiêu bằng cách sử dụng cổng CNOT.

Bước 4: Đo trạng thái của mạch đầu ra

Trường hợp 1: Thực hiện thám hệ mật S-DES khi biết một cặp bản rõ-mã.

Bước 1: Thực hiện tạo cặp bản rõ-mã với khóa cho trước. Với bản rõ p có độ dài 8 bit: p= 00010000 và khóa k = 1100010011. Khi đó, thực hiện mã hóa cho bản rõ p, ta thu được bản mã đầu ra như hình 3.

```
The input plaintext is: 00010000
The input key is: 1100010011
The output from (IP) is the state |00001000> with probability of 1.000000

The output from (XOR1) is the state |11100010> with probability of 1.000000

The output from (P4-R1) is the state |11011000> with probability of 1.000000

The output from (P4-R2) is the state |00101101> with probability of 1.000000

The output ciphertext is: |00110011> with probability of 1.000000

It took 0.000151 seconds to execute
Total time = 0.000147 seconds
```

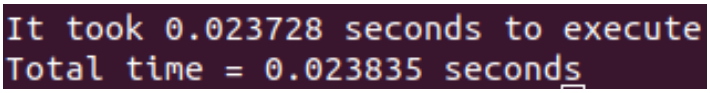
Hình 3. Kết quả bản mã c thu được sau quá trình mã hóa S-DES.

Bước 2: Sử dụng cặp bản rõ-mã tạo được ở Bước 1 với p= 00010000 và khóa c=00110011 để thực hiện tìm khóa k, kết quả sau khi biên dịch và chạy mô phỏng thuật toán Grover tấn công tìm khóa được thể hiện ở hình 4.

```
 0.000726 +0.000000i|7> (5.266659e-07) (|00 0000 0111>)
 0.000726 +0.000000i|11> (5.266656e-07) (|00 0000 1011>)
 0.000726 +0.000000i|51> (5.266676e-07) (|00 0011 0011>)
 0.000726 +0.000000i|83> (5.266749e-07) (|00 0101 0011>)
 0.000726 +0.000000i|147> (5.266638e-07) (|00 1001 0011>)
-0.999728 +0.000000i|787> (9.994553e-01) (|11 0001 0011>)
 0.000726 +0.000000i|2> (5.266659e-07) (|00 0000 0010>)
 0.000726 +0.000000i|4> (5.266659e-07) (|00 0000 0100>)
 0.000726 +0.000000i|5> (5.266658e-07) (|00 0000 0101>)
 0.000726 +0.000000i|6> (5.266659e-07) (|00 0000 0110>)
 0.000726 +0.000000i|8> (5.266659e-07) (|00 0000 1000>)
```

Hình 4. Khóa k của hệ mật S-DES.

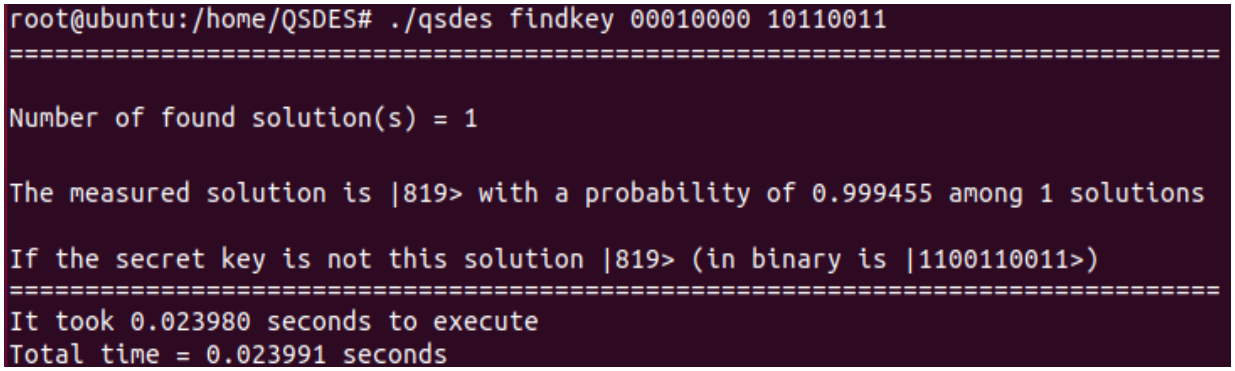
Trong hình 4 cho thấy khóa k tìm được là đúng với khóa k có trong Bước 1 với thời gian tìm khóa của hệ mật S-DES được thể hiện trong hình 5.



Hình 5. Thời gian tìm khóa của hệ mật S-DES.

Trường hợp 2: Thám hệ mật S-DES trong trường hợp sửa đổi đi bản mã với cặp bản rõ-mã đúng.

Với bản rõ p có độ dài 8 bit là p = 00010000 và bản mã c sai = 10110011. Kết quả sau khi chạy mô phỏng là một khóa k sai khác với khóa k có trong Bước 1, trường hợp 1 là k=1110110011 (ở dạng thập phân là: 819), kết quả được thể hiện trong Hình 6.



Hình 6. Khóa của hệ mật S-DES sau khi thử nghiệm với bản mã c sai.

Sau khi thực hiện cài đặt thuật toán tìm kiếm Grover tìm kiếm khóa hệ mật S-DES với kịch bản đầu vào là một cặp văn bản rõ-mã, ta thu được khóa k = 1100110011 với xác suất 0,999455 và thời gian tìm kiếm là 0,023991 giây. Kết quả thử nghiệm được thể hiện ở Bảng 1.

Bảng 1. Kết quả thử nghiệm tấn công với cặp văn bản rõ-mã.

Lần thử nghiệm	**Cặp bản rõ/mã** (p/c)	**Xác suất tìm kiếm khóa thành công** (%)	**Thời gian** (mili giây)
Lần 1	00010000 / 00110011	99,946	23,835
Lần 2	11101100 / 11100000	19,972	14,912
Lần 3	10110001 / 00011100	14,286	12,185

Bảng 2. Chi phí lượng tử của mạch lượng tử đề xuất cho S-AES.

	X-gates	**C-NOT**	**Toffoli**	**Số Qubits**	**Số Qubits Ancilla**
Hàm mở rộng khóa	10	568	192	32	-
Hàm mã hóa	16	512	384	32	8
Tổng số	26	1080	573	64	8

Trong công bố [6],[15],[16] với mã hóa S-AES, việc áp dụng phương pháp nghịch đảo Fermat (thuật toán bình phương và nhân) có thể dẫn đến cùng chi phí tài nguyên về số lượng qubit và cổng lượng tử. Do đó, thuật toán bình phương và nhân được áp dụng để tính ngịch đảo nhân trong trường hữu hạn $GF(2^4)$ của mã hóa S-AES. Mối quan hệ giữa số lượng qubit và cổng lượng tử là nghịch đảo, mặc dù việc sử dụng số lượng qubit trong việc này có thể dẫn đến sự tăng lên số lượng cổng. Theo [16], chi phí lượng tử của mạch lượng tử đề xuất cho S-AES được tính toán và thể hiện trong Bảng 2.

Thuật toán Grover trong công bố [16],[17] đã có các nghiên cứu áp dụng cho tấn công hệ mật S-AES và AES, điều này cho thấy việc áp dụng thuật toán tìm kiếm Grover cho các hệ mật mã khối khác có tính khả thi. Đây là cơ sở cho tác giả tiếp tục nghiên cứu áp dụng thuật toán Grover thám mã cho các hệ mã khối.

4. KẾT LUẬN

Tác giả đã thực thi thuật toán Grover trong thám mã với hệ mật mã khối S-DES, sử dụng tính ưu việt của xử lý tính toán của hàm Oracle và hàm Diffusion làm tăng xác suất tìm kiếm được phần tử đúng, tăng xác suất đo được các trạng thái âm (trạng thái đúng), trong khi giảm xác suất đo được các trạng thái dương. Kết quả đạt được, với ba cặp bản rõ-mã xác định, qua 3 lần thử nghiệm tấn công với thời gian tìm kiếm lần lượt là 23,835 (mili giây), 14,912 (mili giây) và 12,185 (mili giây); xác xuất tìm ra được khóa *k* lần lượt là 99,946%, 19,972% và 14,286%. Đây chính là cơ sở giúp nhóm có các tiền đề để nghiên cứu áp dụng thuật toán tìm kiếm Grover trong việc thám mã với các hệ mật mã khối khác như DES, AES trong tương lai.

LỜI CẢM ƠN

Nghiên cứu này được tài trợ bởi Bộ Giáo dục và Đào tạo trong đề tài mã số đề tài mã số B2025-GHA-02. Tác giả xin chân thành cảm ơn Học viện Kỹ thuật mật mã và Trường Đại học Giao thông vận tải đã hỗ trợ trong quá trình thực hiện nghiên cứu thực nghiệm.

TÀI LIỆU THAM KHẢO

[1]. B. Perez-Garcia, J. Francis, M. McLaren, R. I. Hernandez-Aranda, A. Forbes, T. Konrad, Quantum computation with classical light: The Deutsch Algorithm, Phys. Lett. A, 379 (2015) 1675–1680. https://doi.org/10.1016/j.physleta.2015.04.034

[2]. I. B. Djordjevic, Quantum Information Processing, Quantum Computing, and Quantum Error Correction: An Engineering Approach, Second Edi. Elsevier, 2021.

[3]. M. Schwetz, R. M. Noack, Simon algorithm in measurement-based quantum computing, 2024. http://arxiv.org/abs/2405.18143

[4]. C. Guo, Grover's Algorithm – Implementations and Implications, Highlights Sci. Eng. Technol., 38 (2023) 1071–1078. https://doi.org/10.54097/hset.v38i.5997

[5]. D. Camps, R. Van Beeumen, C. Yang, Quantum Fourier transform revisited, Numer. Linear Algebr. with Appl., 28 (2021). https://doi.org/10.1002/nla.2331

[6]. D. V. Denisenko, M. V. Nikitenkova, Application of Grover's Quantum Algorithm for SDES Key Searching, J. Exp. Theor. Phys., 128 (2019) 25–44. https://doi.org/10.1134/S1063776118120142

[7]. D. V. Lữ, H. P. Anh, H. B. Nguyên, N. N. M. Trí, C. T. M. Hảo, N. T. Hồng, Nghiên cứu ứng dụng thuật toán lượng tử Grover trong giải trình tự DNA, TNU J. Sci. Technol., 229 (2024) 65–72. https://doi.org/10.34238/tnu-jst.9932

[8]. E. F. Schaefer, A Simplified Data Encryption Standard Algorithm, Cryptologia, 20 (1996) 77–84. https://doi.org/10.1080/0161-119691884799

[9]. D. R. Stinson, Cryptography, Third Edit. Chapman and Hall/CRC, 2005.
[10]. R. Awadallah, A. Samsudin, M. Almazrooie, Verifiable Homomorphic Encrypted Computations for Cloud Computing, Int. J. Adv. Comput. Sci. Appl., 12 (2021). https://doi.org/10.14569/IJACSA.2021.0121089
[11]. M. Almazrooie, A. Samsudin, R. Abdullah, K. N. Mutter, Quantum exhaustive key search with simplified-DES as a case study, Springerplus, 5 (2016) 1494. https://doi.org/10.1186/s40064-016-3159-4.
[12]. L. Nhu Quynh, L. Van Anh, Implement quantum random number generation on the IBM quantum computer platform, Transp. Commun. Sci. J., 75 (2024) 1644–1658. https://doi.org/10.47869/tcsj.75.4.14
[13]. A. Javadi-Abhari, M. Treinish, K. Krsulich, C. J. Wood, J. Lishman, J. Gacon, S. Martiel, P. D. Nation, L. S. Bishop, A. W. Cross, B. R. Johnson, J. M. Gambetta, Quantum computing with Qiskit, (2024). http://arxiv.org/abs/2405.08810
[14]. M. Fingerhuth, T. Babej, P. Wittek, Open source software in quantum computing, PLoS One, 13 (2018) e0208561. https://doi.org/10.1371/journal.pone.0208561
[15]. K.-B. Jang, G.-J. Song, H.-J. Kim, H.-J. Seo, Grover on Simplified AES, 2021 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia), 2021, IEEE, pp. 1–4. https://doi.org/10.1109/ICCE-Asia53811.2021.9642017
[16]. M. Almazrooie, R. Abdullah, A. Samsudin, K. N. Mutter, Quantum Grover Attack on the Simplified-AES, Proceedings of the 2018 7th International Conference on Software and Computer Applications, 2018, New York, USA: ACM, pp. 204–211. https://doi.org/10.1145/3185089.3185122
[17]. S. Mandal, R. Anand, M. Rahman, S. Sarkar, T. Isobe, Implementing Grover's on AES-based AEAD schemes, Sci. Rep., 14 (2024) 21105. https://doi.org/10.1038/s41598-024-69188-8