Variational Quantum Attacks on Symmetric-Key Ciphers

Anand Kasyup — EP22BTECH11012
Edara Yaswanth Balaji — EP22BTECH11007

Project Supervisor: Prof. M. V. Panduranga Rao

Project co-guide: Prof. Archak Purkayastha

Department of Physics
Indian Institute of Technology Hyderabad

భారతీయ సాంకేతిక విజ్ఞాన సంస్థ హైదరాబాద్
भारतीय प्रौद्योगिकी संस्थान हैदराबाद
Indian Institute of Technology Hyderabad

Abstract

We studied a variational quantum attack algorithm (VQAA) for classical AES-like symmetric cryptography, as exemplified the simplified-data encryption standard (S-DES). In the VQAA, the known ciphertext is encoded as the ground state of a Hamiltonian that is constructed through a regular graph, and the ground state can be found using a variational approach. A classical optimiser steers circuit angles so that the measured ciphertext overlaps the target state, causing the key register to collapse to the correct 10-bit key. As Noisy-intermediate-scale quantum (NISQ) processors demand hybrid workflows that keep quantum circuits shallow while off-loading heavy optimisation to classical hardware. We adopt this strategy in a **Variational Quantum Attack Algorithm** (VQAA).

Building on this baseline, we also studied an **improved VQAA** that executes encryption classically after an early measurement. A brick-wall *U–CNOT* ansatz plus multi-start warm-up and early stopping avoids barren plateaux and accelerates convergence. Our results show that carefully chosen ansätze, cost functions and optimiser heuristics can potentially yield quantum speed-ups for symmetric-key cryptanalysis and they set the stage for more research on scaling such attacks.

Contents

1 Introduction 2

1.1 Quantum Computing 2

1.2 Variational Quantum Algorithms 2

2 Cryptographic Background 3

2.1 Symmetric-Key Setting 3

2.2 Why S-DES? 3

3 VQAA Algorithm 4

3.1 Circuit 4

3.2 Y–C_z Staircase Ansatz 5

3.3 Cost Function Hamiltonian 5

3.4 Classical Optimizers 6

3.5 Full quantum circuit Implementation on Qiskit 7

3.6 Issues with the VQAA 7

4 Improved VQAA 8

4.1 New Ansatz 8

4.2 Initialization Strategy 8

4.3 Execution Results and Observations 9

5 Conclusion and Future Work 10

1 Introduction

Modern communication relies on symmetric ciphers such as AES. Quantum search algorithms jeopardise these ciphers in principle, yet fully fault-tolerant machines remain decades away. NISQ hardware therefore motivates *Variational Quantum Algorithms* , which iterate between a short quantum circuit and a classical optimizer. Established examples include the Variational Quantum Eigensolver

This study adapts the same hybrid idea to cryptanalysis by applying a Variational Quantum Algorithm to the key search problem in symmetric-key cryptography, focusing on S-DES as a case study. Section 3 reviews the baseline Variational Quantum Attack Algorithm (VQAA) and Section 4 presents an improved version better aligned with NISQ constraints. We tried to implement both on S-DES.

1.1 Quantum Computing

Quantum computing is based on the principles of quantum mechanics, specifically superposition, entanglement, and quantum interference. Unlike classical bits, quantum bits (or qubits) can exist in a superposition of states, meaning they can represent both 0 and 1 simultaneously. This property allows quantum computers to perform many calculations in parallel. Additionally, qubits can become entangled, which means the state of one qubit is inherently linked to the state of another, regardless of the distance between them. Quantum circuits are built using quantum gates, represented by unitary matrices that manipulate qubit states. Quantum operations are probabilistic in nature, meaning that upon measurement, the outcome is not deterministic but rather occurs with a certain probability distribution.

1.2 Variational Quantum Algorithms

Variational Quantum Algorithms (VQAs) are hybrid methods designed specifically for today's noisy-intermediate-scale-quantum (NISQ) processors. They operate in a closed loop: a shallow, parameterised quantum circuit prepares a trial state; the device is measured; and a classical optimiser adjusts the circuit's angles so that a chosen cost function steadily decreases. This synergy allows the quantum hardware to explore an exponentially large state space while the classical computer performs the heavy numerical search.

Two landmark VQAs highlight the idea:

- **Variational Quantum Eigensolver (VQE)** – Targets chemistry and materials science by minimising the expectation value of a molecular Hamiltonian, thereby approximating its ground-state energy. The ansatz is often chemically inspired, and only a few circuit layers are needed to achieve useful accuracy.
- **Quantum Approximate Optimisation Algorithm (QAOA)** – Tackles discrete optimisation problems such as Max-Cut. It alternates problem-specific phase operators with mixing operators, tuning their rotation angles so that repeated measurements yield solutions with high objective-function values.

Because all quantum subroutines remain shallow, VQAs tolerate short coherence times and modest gate fidelity. Meanwhile, the classical optimiser compensates for noise by steering the parameters toward regions of the landscape that are both low in cost and robust against device imperfections. This hybrid strategy has therefore become the workhorse for practical quantum computing in the NISQ era.

2 Cryptographic Background

2.1 Symmetric-Key Setting

- **Single shared key**
  One secret key K is used for *both* encryption and decryption:
  $$C = E_K(P), \qquad P = D_K(C),$$
  where P is the plaintext and C the ciphertext.
- **Public algorithm**
  Every detail of the algorithm E is assumed known to the adversary (Kerckhoffs' principle). Security rests entirely on the secrecy and bit-length of K.
- **Computational security**
  A cipher is considered secure if recovering K requires a brute-force search over $2^{|K|}$ keys, which is infeasible on classical hardware for $|K| \geq 128$ but becomes vulnerable once quantum search (e.g. Grover) reduces complexity to $\mathcal{O}(2^{|K|/2})$.
- **Key-search complexity**
  Exhaustive classical search scales as $\mathcal{O}(2^{|K|})$; early fault-tolerant quantum computers would cut this to $\mathcal{O}(2^{|K|/2})$, motivating hybrid NISQ attacks such as the VQAA studied here.

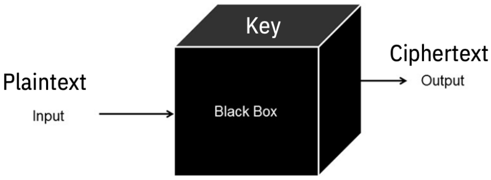

Figure 1: Black-box view of a symmetric cipher. The attacker controls plaintext input and observes ciphertext output.

2.2 Why S-DES?

The **Simplified Data Encryption Standard** (S-DES) is an instructional cipher that distils the original 64-bit DES into an 8-bit block size with a 10-bit secret key. Despite its reduced scale, it preserves the essential DES structure:

- a two-round *Feistel network* that splits the block into left and right halves,
- key-dependent *S-boxes* that introduce non-linearity, and
- fixed *permutation* layers that diffuse bit positions.

This downsizing keeps the full key space at $2^{10} = 1024$ possibilities, small enough for classical brute force yet large enough to demonstrate quantum speed-ups. Moreover, the 8-qubit plaintext and 10-qubit key map neatly onto present-day simulators and mid-scale hardware, allowing us to prototype and benchmark variational attacks end-to-end. Figure 2 summarises one encryption pass, highlighting the round keys K_1 and K_2 derived from the master key.

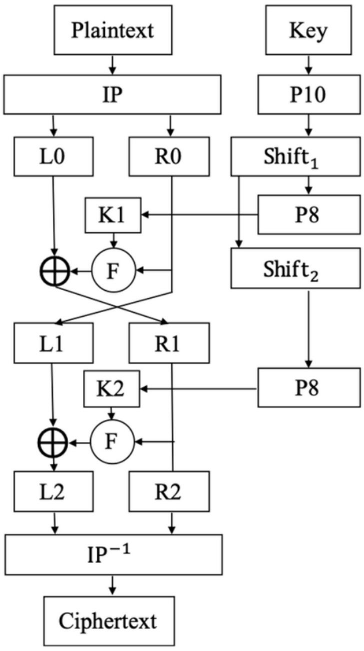

Figure 1 The encryption process of S-DES.

Figure 2: Encryption flow of S-DES. Two sub-keys K_1 and K_2 feed the round function f.

3 VQAA Algorithm

3.1 Circuit

1. **Hamiltonian set-up** – From the known plaintext–ciphertext pair we build a cost Hamiltonian whose ground state is the ciphertext.
2. **Ansatz preparation** – A 10-qubit key register is driven by a parametrised circuit, creating a superposition over all 2^{10} keys; an 8-qubit data register holds the plaintext.
3. **Quantum encryption** – Passing both registers through the reversible S-DES oracle yields a superposition of candidate ciphertexts entangled with their keys.
4. **Measurement & update** – Measuring the data qubits gives one ciphertext sample. A classical optimiser then adjusts the circuit parameters so that amplitude shifts toward the target ciphertext (lowest-energy state).

When the sampler finally returns the correct ciphertext, the key register collapses to the desired 10-qubit key—completing the attack. Dashed lines in Fig. 3 separate the quantum routine (left) from the classical optimisation loop (right).

A concise flow is as follows:

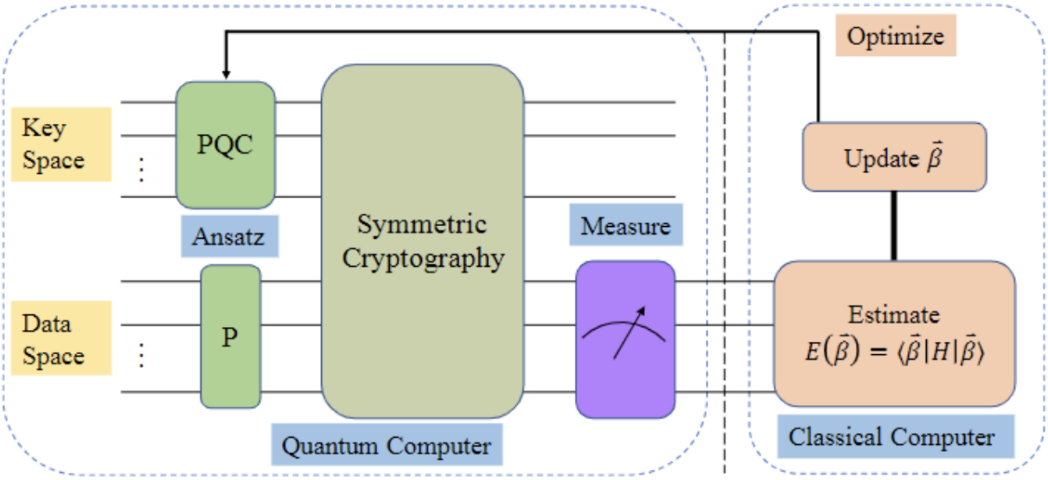

Figure 3: Control flow of the original VQAA [4]).

3.2 Y–C_z Staircase Ansatz

A single-layer ansatz

1. **Initialization:** each key qubit, initialized as $|0\rangle$ enters $|+\rangle$ via H;
2. **Parameterized layer:** apply $R_y(\theta_i)$ to create a weighted superposition of 0 and 1;
3. **Entanglement ladder:** nearest-neighbour C_z gates spread correlations;
4. **Biasing hook:** a final wrap-around C_z can amplify overlap with promising key regions.

This ansatz prioritizes entangling neighboring qubits to capture local correlations in the key space. The layer uses n parameters and depth $n + 2$.

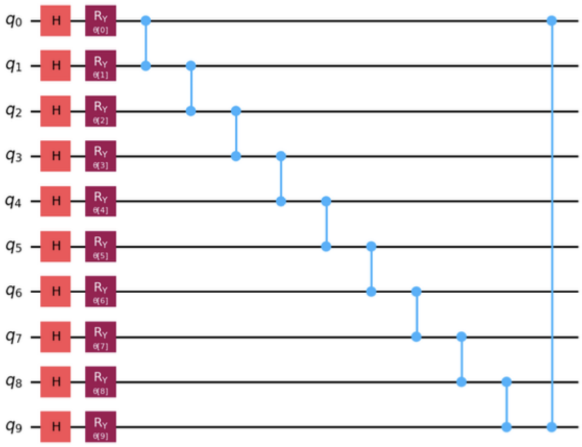

Figure 4: Single-layer Y–CZ ansatz for $n = 10$ qubits.

3.3 Cost Function Hamiltonian

Following [4], we encode the target ciphertext as the ground state of an Ising Hamiltonian on a 3-regular graph (Fig. 5). All terms commute, enabling single-shot energy estimation, which reduces the number of circuit evaluations needed to estimate the cost function.

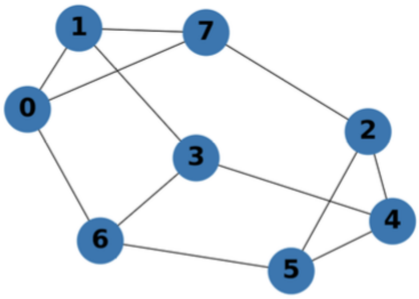

Figure 5: 3-regular graph ($n = 8$) used in the cost Hamiltonian.

We consider the following cost function Hamiltonian H, constructed using Pauli-Z interactions between qubits:

$$\begin{aligned} H = {} & w_{01}Z_0Z_1 + w_{06}Z_0Z_6 + w_{07}Z_0Z_7 + w_{13}Z_1Z_3 + w_{17}Z_1Z_7 \\ & + w_{24}Z_2Z_4 + w_{25}Z_2Z_5 + w_{27}Z_2Z_7 + w_{34}Z_3Z_4 + w_{36}Z_3Z_6 \\ & + w_{45}Z_4Z_5 + w_{56}Z_5Z_6 + \sum_{i=0}^{7} t_i Z_i \end{aligned}$$

The weights are defined by:

$$w_{ij} = \begin{cases} 1 & \text{if } V(i) \neq V(j) \\ -1 & \text{if } V(i) = V(j) \end{cases} \qquad t_i = \begin{cases} 0.5 & \text{if } V(i) = 1 \\ -0.5 & \text{if } V(i) = 0 \end{cases}$$

where $V(i)$ is the i-th bit of the ciphertext.

This ensures that the correct ciphertext has the least expectation value when the Hamiltonian measurement is performed.

3.4 Classical Optimizers

We tested three different optimization algorithms which are Gradient Descent, Adam Optimizer and COBYLA (Constrained Optimization By Linear Approximation).
Gradient descent worked the best in terms of faster convergence.

3.5 Full quantum circuit Implementation on Qiskit

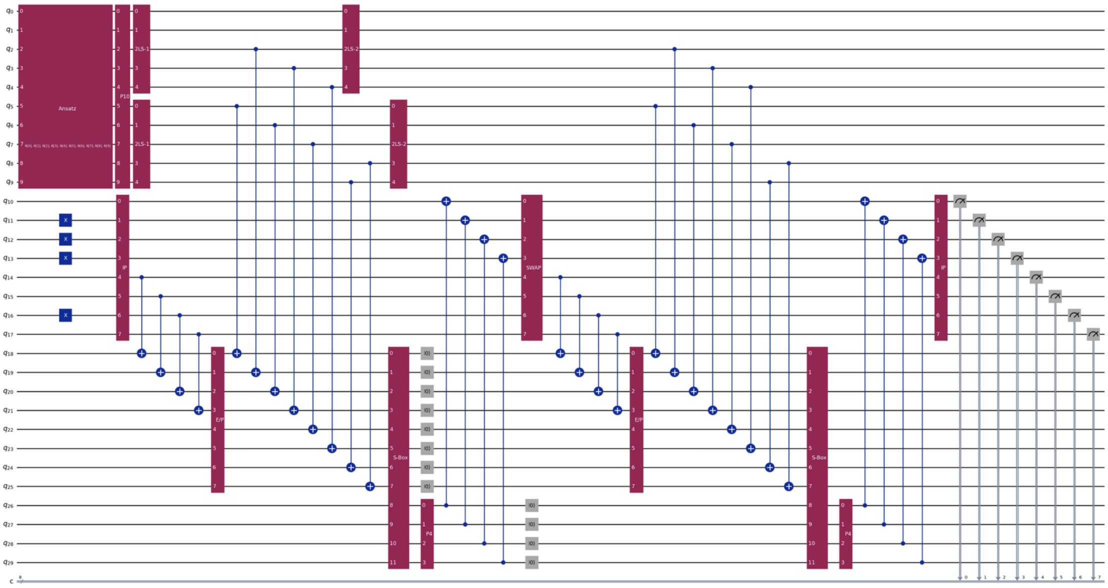

Figure 6: Complete circuit diagram as implemented on Qiskit

3.6 Issues with the VQAA

A 30-qubit experiment on `ibm_sherbrooke` exposed long queue times, noisy cost estimates, and optimizer stagnation, a wakeup call for a leaner approach.

1. **High Qubit Count:** Our implementation required 30 qubits, exceeding the practical limits of classical simulation. Such a large-scale system is prone to significant quantum noise, making near-term execution unreliable.

2. **Optimisation struggles:** VQAA relies on classical optimizers, but: They can stall in barren plateaus — flat regions in the loss landscape where gradients vanish. Initial parameter selection is critical, yet there is no heuristic guidance available for effective initialization.

3. **Ansatz sensitivity:** The performance of VQAA is very dependent on the ansatz. A poorly chosen ansatz can restrict expressibility and convergence. We identified and implemented a tailored ansatz, which significantly improved performance and stability.

4 Improved VQAA

The refined algorithm in Aizpurua et al., [5] tackles each obstacle head on.

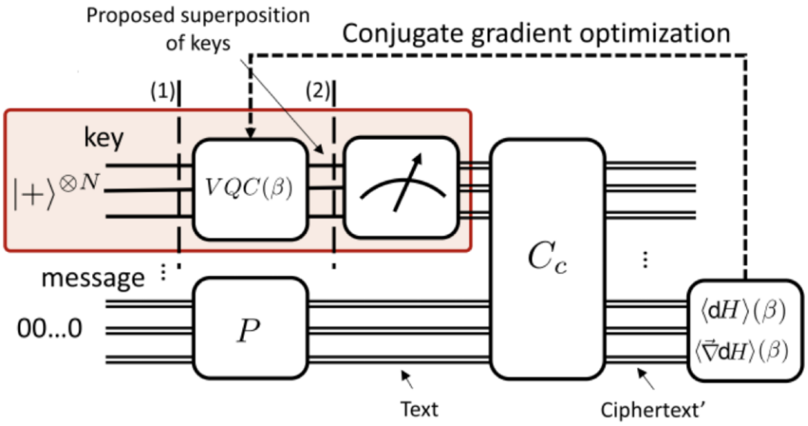
Proposed superposition of keys
Conjugate gradient optimization
(1)
(2)
key
$|+\rangle^{\otimes N}$
$VQC(\beta)$
message
00...0
P
C_c
$\langle dH\rangle(\beta)$
$\langle\vec{\nabla} dH\rangle(\beta)$
Text
Ciphertext'

Figure 7: High-level structure of the improved VQAA. Only the red box is executed on the quantum processor. The reversible S-DES Encrytion is removed. Encryption runs classically after measuring the key register

4.1 New Ansatz

A different approach on implementing the ansatz circuit using the U–C_{NOT} gates to have a better chance at faster convergence

1. **Initialisation**: Hadamards place all qubits in $|+\rangle$.
2. **Parameterized layer**: universal $U(\theta, \phi, \lambda)$ rotations enable arbitrary single-qubit states.
3. **Entanglement**: a forward C_{NOT} cascade ($q_i \to q_{i+1}$) encodes correlations.
4. **Efficiency**: the circuit explores key space effectively without increasing depth.

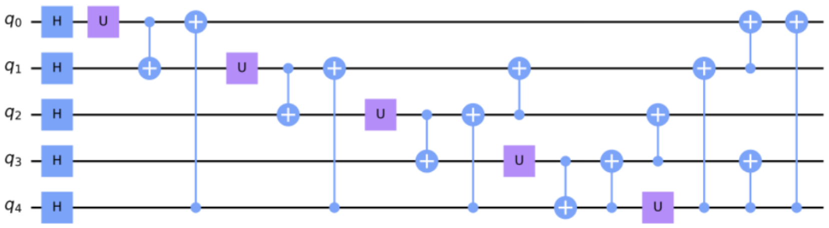

Figure 8: Enhanced ansatz using $U(\theta, \phi, \lambda)$ gates and linear C_{NOT} entanglement.

4.2 Initialization Strategy

- **Initialisation**: Sample ten sets of random parameters $\{\theta^{(k)}\}_{k=1}^{10}$.
- **Local search**: Run gradient descent for ten steps with learning rate 0.1; stop if $\|\nabla E\| < 10^{-6}$.
- **Selection**: Choose the seed(params) with the lowest cost for the full optimization run.

This strategy mitigates poor initialization and accelerates convergence by avoiding barren plateaus.

4.3 Execution Results and Observations

- The Improved VQAA successfully recovered the correct S-DES key *1010000010*, for a plaintext(*10010111*), ciphertext(*00111000*) pair achieving a final cost of Emin=17.08, outperforming baseline VQAA (Emin 13.7).

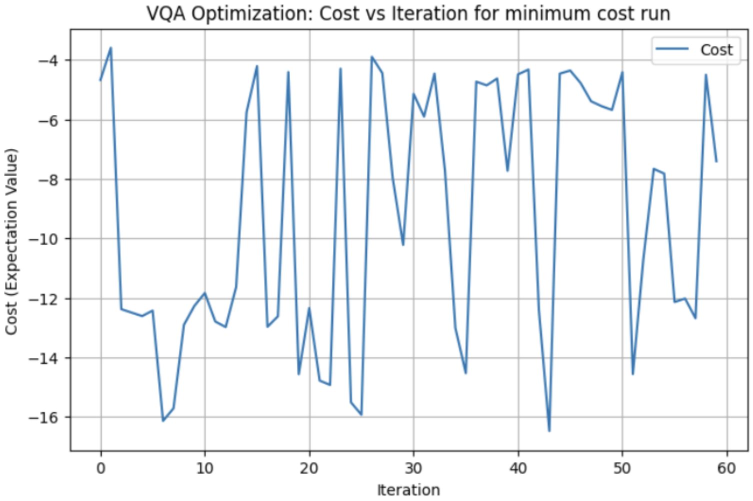

Figure 9: Improved VQAA Cost versus iteration for the lowest-cost run.

- Among 1024 bitstring samples, the correct key appeared 231 times, within the top 4 outputs accounting for 96.8% of counts.
- Using multi-start warm-up with early stopping (E ¡ 106), optimization avoided barren plateaus and converged reliably.

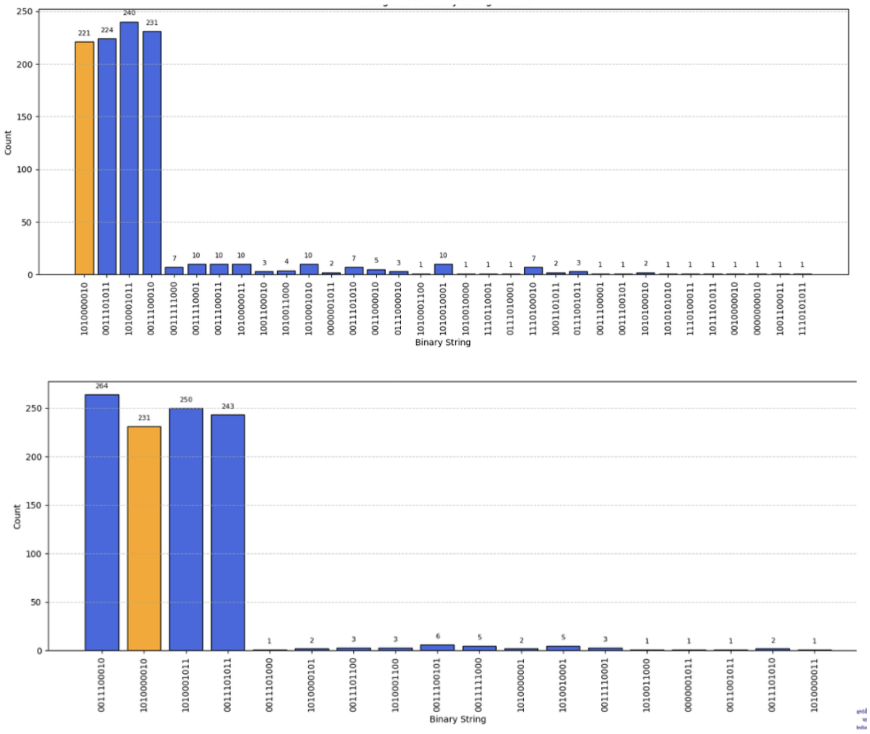

Figure 10: Bit-string frequency after 1024 samples for two optimiser seeds. Orange bar represents target key.

Overall, the improved design offers better key-space exploration, faster convergence and higher success probability while using less than half the qubits needed for Baseline VQAA.

5 Conclusion and Future Work

The main ideas for circuit implementation were from the cited papers but we needed to implement all of the circuits from scratch for thee algorithm analysis. For the Cost function and Ansatz, we considered a lot of options and chose the best one after implementing and comparing the performance While universal convergence is unproven, customising the cost function and optimiser for each plaintext–ciphertext pair can still promise good results. Our work lays a solid foundation for quantum cryptanalysis of symmetric ciphers and can provide further studies with a better starting point.

References

[1] A. Biryukov and A. Shamir, *Cryptanalysis of S-DES.* Cryptology ePrint Archive, Report 2002/044, 2002.

[2] "The complexity of NISQ," *Nature Communications* 14, 2023.

[3] R. Somma *et al.*, "The Variational Quantum Eigensolver: a review of methods and best practices," *arXiv*:2108.03993, 2021.

[4] Z. Wang, S. Wei, G.-L. Long and L. Hanzo, "A Variational Quantum Attack for AES-like Symmetric Cryptography," *arXiv*:2205.03529, 2022.

[5] B. Aizpurua, P. Bermejo, J. Etxezarreta Martínez and R. Orús, "Hacking Cryptographic Protocols with Advanced Variational Quantum Attacks," *ACM Trans. Quantum Comput.* 6(2):14, 2025.

[6] J. Preskill, "Quantum Computing in the NISQ era and beyond," *Quantum* 2, 79 (2018).

===