Variational Quantum Attack for Symmetric Cryptographic Systems

Edara Yaswanth Balaji | Kurella Anand Kasyup
EP22BTECH11007 | EP22BTECH11012
Indian Institute of Technology, Hyderabad

Abstract

In the era of NISQ (Noisy Intermediate-Scale Quantum) hardware, Quantum-Classical hybrid Algorithms have become the need of the hour. Hence we explore an application of one such class of algorithms, Variational Quantum Algorithms (VQAs). We explored the use of a VQA to try and break Symmetric key ciphers, and as a primer, we tried breaking the S-DES cryptographic system.

In the VQAA, the known ciphertext is encoded as the ground state of a Hamiltonian,and the ground state can be found using a variational approach. We designed the ansatz and cost function for the S-DES's variational quantum attack.

S-DES

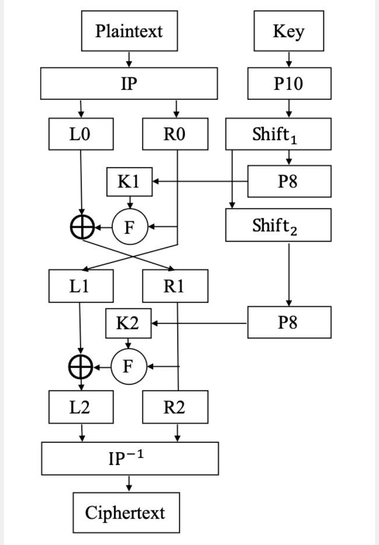


Figure 1. Encryption flow of S-DES

Encryption:

$$\text{Ciphertext} = IP^{-1} \circ f_{K_2} \circ SW \circ f_{K_1} \circ IP(\text{Plaintext})$$

Decryption:

$$\text{Plaintext} = IP^{-1} \circ f_{K_1} \circ SW \circ f_{K_2} \circ IP(\text{Ciphertext})$$

Variational Quantum Workflow

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

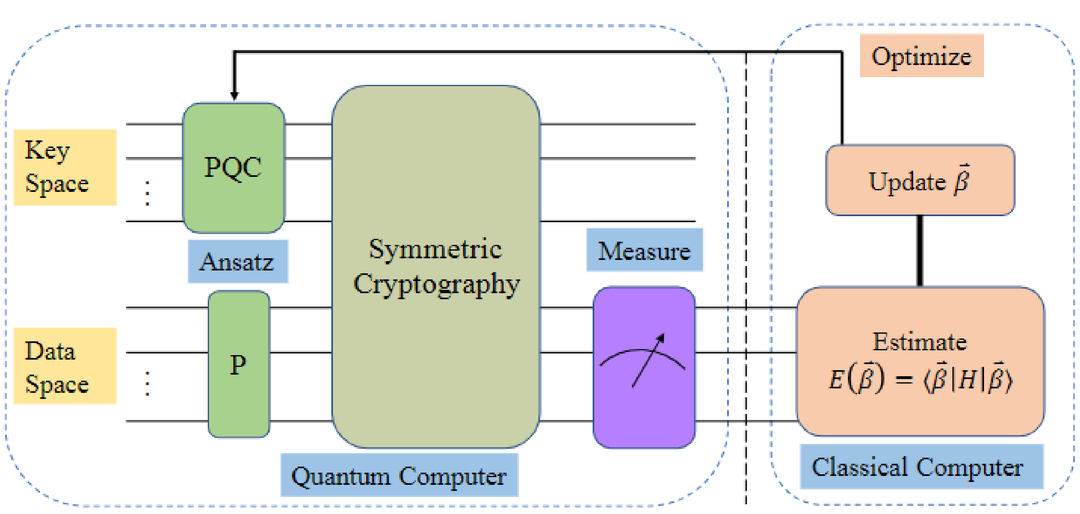


Figure 2: Schematic diagram of the quantum attack on S-DES using VQAs, where β represents the parameters of PQC

Ansatz

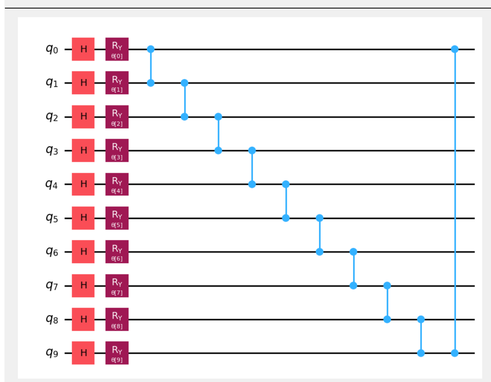


Figure 1. Parameterized ansatz circuit preparing a superposition over all key states

Y-C$_z$ Ansatz (Single Layer)

- *Initialization*: Each key qubit is placed in a parameterized state using H followed by $R_y(\theta_i)$, generating a weighted superposition of 0 and 1.
- *Superposition*: This creates a quantum state that encodes a distribution over all 2^n possible keys, with amplitudes determined by the parameters $\boldsymbol{\theta}$.
- *Entanglement*: A nearest-neighbour controlled gates spread correlations across qubits to allow non-separable key distributions.
- *Biasing Hook*: A final controlled-Z (multi-CZ) operation can amplify overlap with target keys by shifting the global phase.
- *Circuit Depth*: Uses n parameters with circuit depth $\approx n{+}2$ (e.g., depth = 12 for 10-qubit S-DES).

Cost Function 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.

Classical Optimizers

The algorithms we tested are Gradient Descent, N-M method, COBYLA.
Gradient descent worked the best in terms of faster convergance.

Issues with VQAA

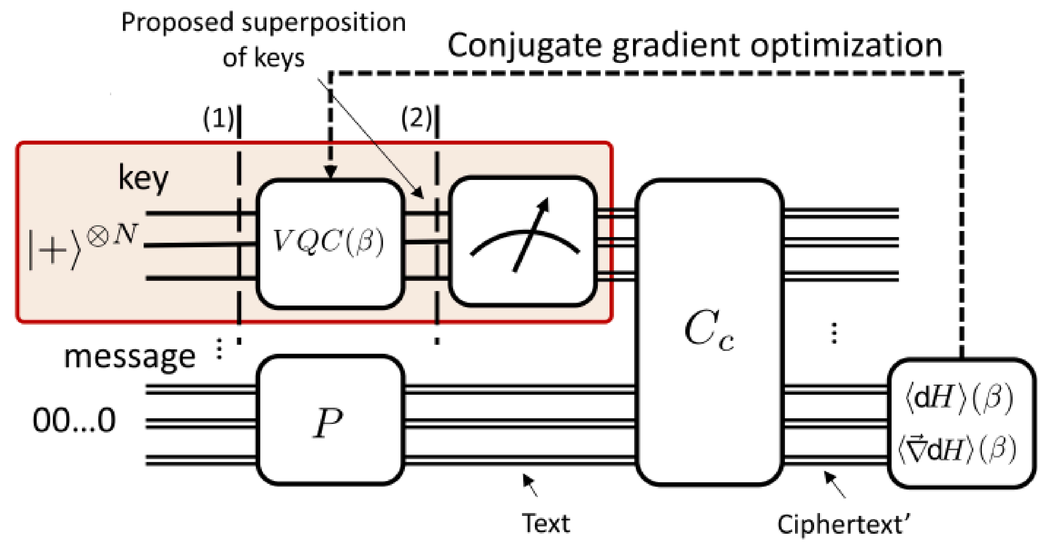
1. **High Qubit Count Limits Simulation:** Our implementation required 39 qubits, exceeding the practical limits of classical simulation. Such a large-scale system is prone to significant quantum noise, making near-term execution unreliable.

2. **Optimization 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.

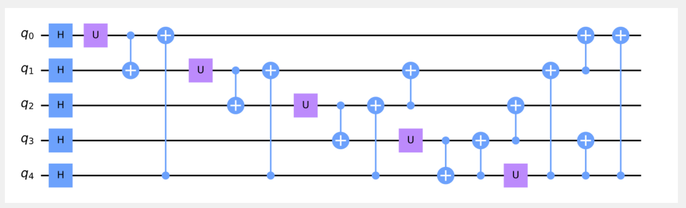
3. **Ansatz Sensitivity:** The performance of VQAA is very dependent on the ansatz. A poorly chosen ansatz can restrict expressibility and convergence. We identified and implemented a tailored ansatz, which significantly improved performance and stability.

Improved VQAA

[2] B. Aizpurua, P. Bermejo, J.Etxezarreta Martínez, and R.Orús, Hacking Cryptographic Protocols with Advanced Variational Quantum Attacks, arXiv:2311.02986 [quant-ph], March, 2025.



New Ansatz



Improved Ansatz (Single Layer)

- *Initialization:* All qubits are placed in the + state via Hadamard gates
- *Parameterized Layer:* A layer of single-qubit $U(\theta, \phi, \lambda)$ gates allows arbitrary rotations on the Bloch sphere, enabling full expressivity.
- *Entanglement:* Forward CNOT cascade ($q_i \rightarrow q_{i+1}$) couples neighboring qubits to encode correlations.
- *Efficiency:* Offers improved key-space exploration while maintaining similar or slightly reduced iteration counts compared to the previous ansatz setups.

Figure 2. Structure of the enhanced ansatz using general $U(\theta, \phi, \lambda)$ gates and linear CNOT entanglement. This form improves flexibility for parameter optimization without increasing circuit depth significantly.

Optimization and Execution

Multi-start warm-up with early stopping

- **Initialisation:** Sample 10 random parameter sets $\{\boldsymbol{\theta}^{(k)}\}_{k=1}^{10}$, each of shape $2{\times}10$ over $[0, 2\pi]$.
- **Local search:** For each, run gradient descent for up to 10 iterations with learning rate 0.1 and convergence threshold $\|\nabla E\| < 10^{-6}$.
- **Selection:** The best seed $\boldsymbol{\theta}^\star = \arg\min_k E^{(k)}$ is used for the final execution phase.

This strategy reduces the risk of poor initialisation and accelerates convergence by avoiding barren plateaus.

Results & Contribution

- The Improved VQAA successfully recovered the correct S-DES key `1010000010`, for a plaintext(`10010111`), ciphertext(`00111000`) pair achieving a final cost of $E_{\text{min}} = -17.08$, outperforming baseline VQAA ($E_{\text{min}} \approx -13.7$). Using multi-start warm-up with early stopping ($\|\nabla E\| < 10^{-6}$), optimization avoided barren plateaus and converged reliably.
- Among 1024 bitstring samples, the correct key appeared 231 times, within the top 4 outputs accounting for 96.8% of counts.
- The main ideas for circuit implementation were from the cited papers but we needed to implement all of them from scratch on our own. We believe that we had come up with the most optimal code for the proposed algorithm.
- 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 more studies can be done on this.

References

1. Z. Wang, S. Wei, G.-L. Long, and L. Hanzo, *A Variational Quantum Attack for AES-like Symmetric Cryptography*, arXiv:2205.03529 [quant-ph], 2022.
2. B. Aizpurua, P. Bermejo, J.Etxezarreta Martínez, and R.Orús, *Hacking Cryptographic Protocols with Advanced Variational Quantum Attacks*, arXiv:2311.02986 [quant-ph], March, 2025.

ep22btech11007@iith.ac.in | ep22btech11012@iith.ac.in