Quantum Attacks for Symmetric Crypto Systems

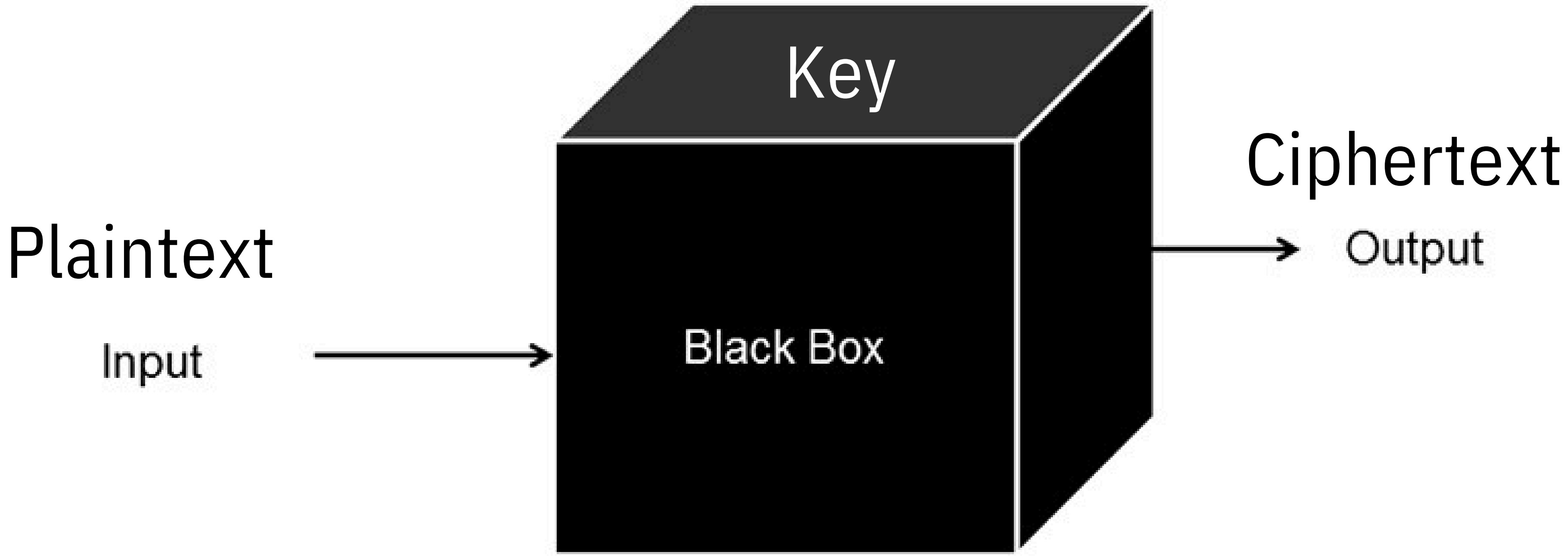
Anand Kasyup - EP22BTECH11012
Anirudh Saikrishnan - CS22BTECH11001
Yaswanth Balaji - EP22BTECH11007

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

Cryptography

Symmetric Key Cryptography

- Same secret key is used to both encrypt and decrypt messages.
- We know the complete algorithm
- We have access to a black box with the key and the algorithm embedded



S-DES

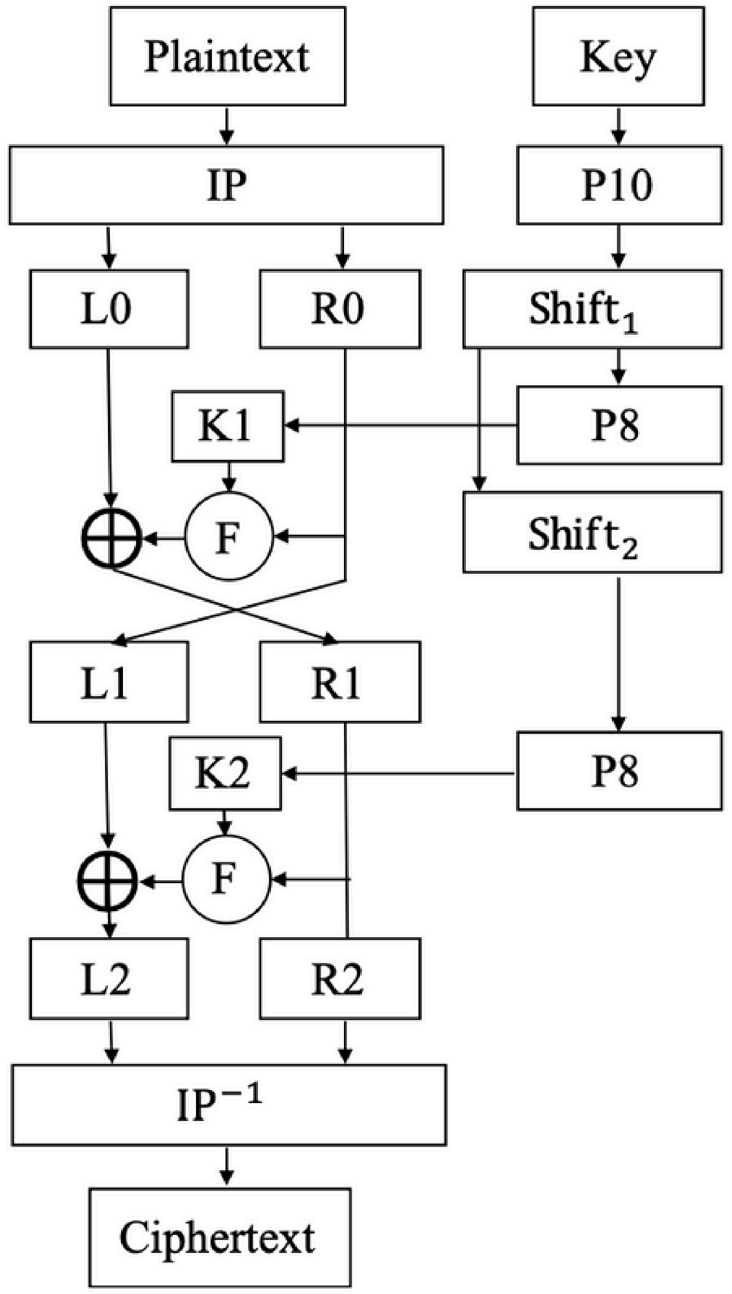


Figure 1 The encryption process of S-DES.

- 8-bit block cipher with a 10-bit key
- Encryption:
  - Ciphertext = $IP^{-1} \circ f(K_2) \circ SW \circ f(K_1) \circ IP(\text{Plaintext})$
- Decryption:
  - Plaintext = $IP^{-1} \circ f(K_1) \circ SW \circ f(K_2) \circ IP(\text{Ciphertext})$
- The most efficient classical algorithm to break S-DES
  - Brute-force attack [1]

[1] Biryukov, A., & Shamir, A. (2002). Cryptanalysis of S-DES. Cryptology ePrint Archive

Overview

The Algorithms we are going to discuss:

1. VQAA for S-DES
2. Grovers for S-DES
3. Improved VQAA for S-DES (brief)

Current Quantum Era

- NISQ hardware [2]
  - Only tens of qubits
  - Low gate fidelities and shallow-depth circuits
- Hybrid quantum–classical algorithms were developed to work within these NISQ limitations
- Such methods excel at combinatorial optimization and finding Hamiltonian ground states, with applications in quantum chemistry, machine learning, and finance.
  - VQE [3] - quantum chemistry
  - QAOA [4] - optimization

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

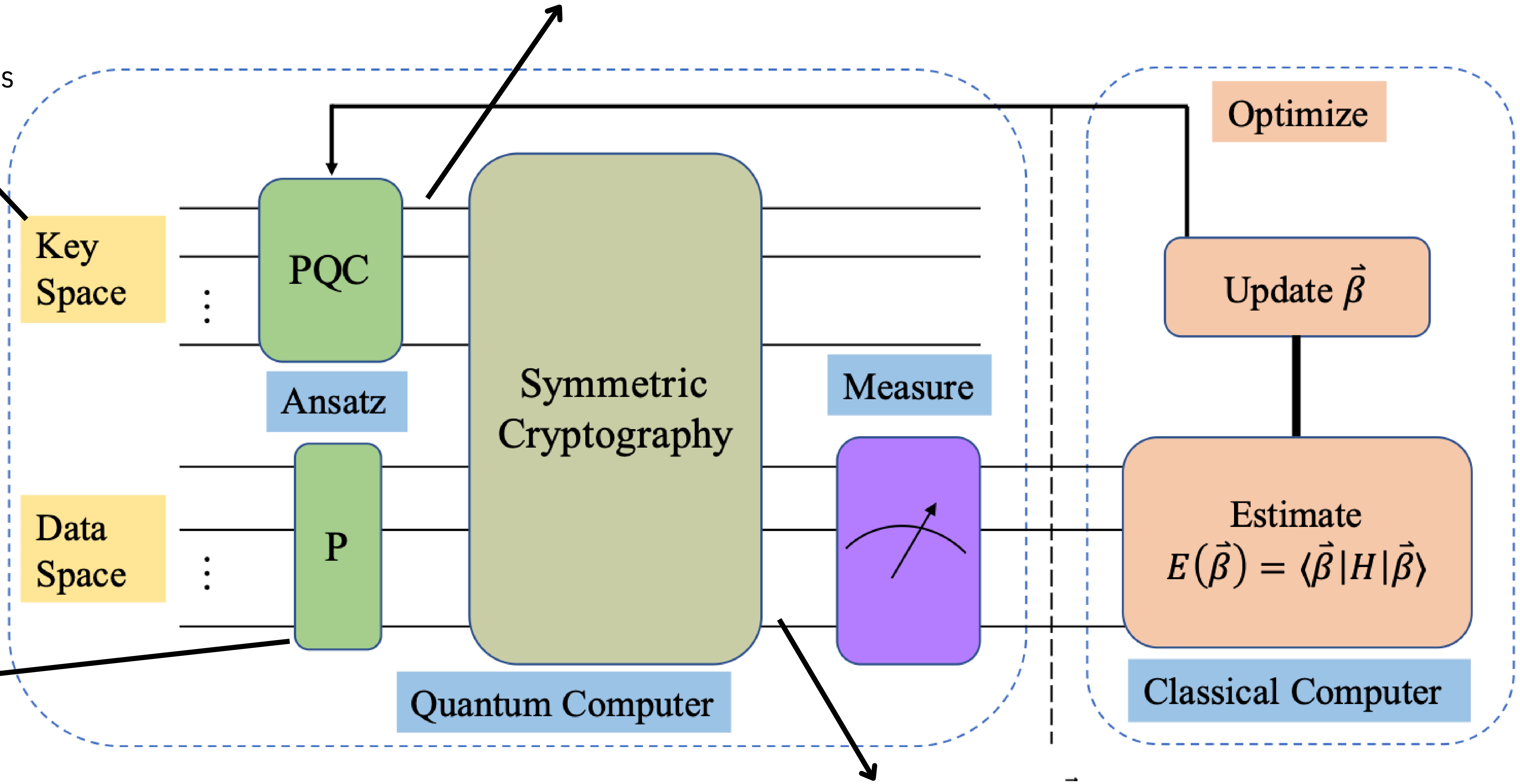
[3] The Variational Quantum Eigensolver: a review of methods and best practices. arXiv preprint arXiv:2108.03993, 2021. arXiv

[4] The Quantum Approximate Optimization Algorithm and the Sherrington–Kirkpatrick Model. Quantum, 2022. Quantum Journal

VQAA Circuit

A random superposition state depending on the parameters

Initialised as all zeroes



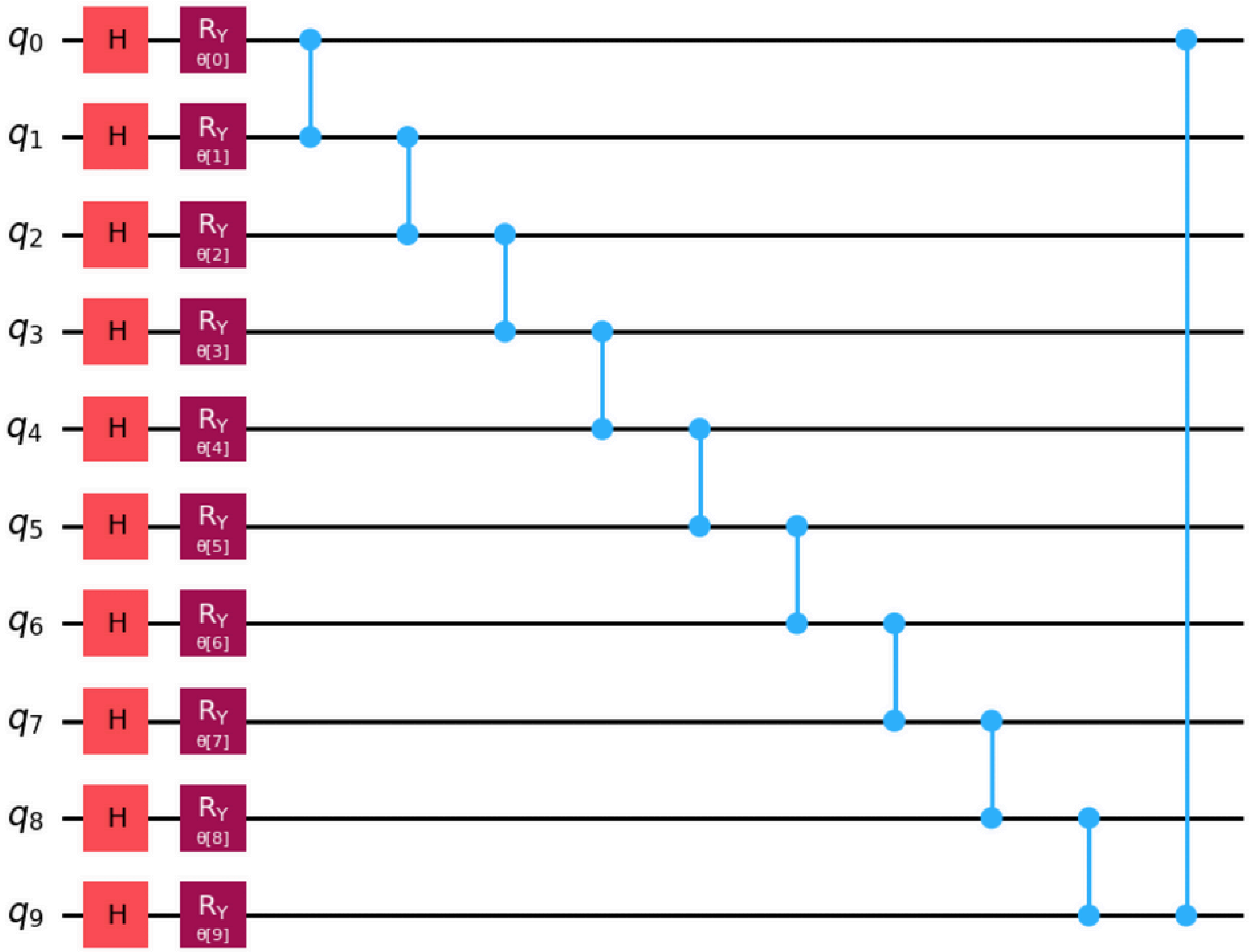
Encoding the plaintext using X gates

A random superposition of ciphertexts

When we measure, we get one of the ciphertexts as output which corresponds to one of the keys. Our goal is to optimize the PQC to get the known cipher text when we measure

[5] A Variational Quantum Attack for AES-like Symmetric Cryptography. ZeGuo Wang, ShiJie Wei, Gui-Lu Long & Lajos Hanzo.

Ansatz



- 1-layer of ansatz requires n parameters
- circuit depths is n+2
- Gate Z represents a Pauli-Z gate

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

- Ry gate is a rotation gate with a parameter

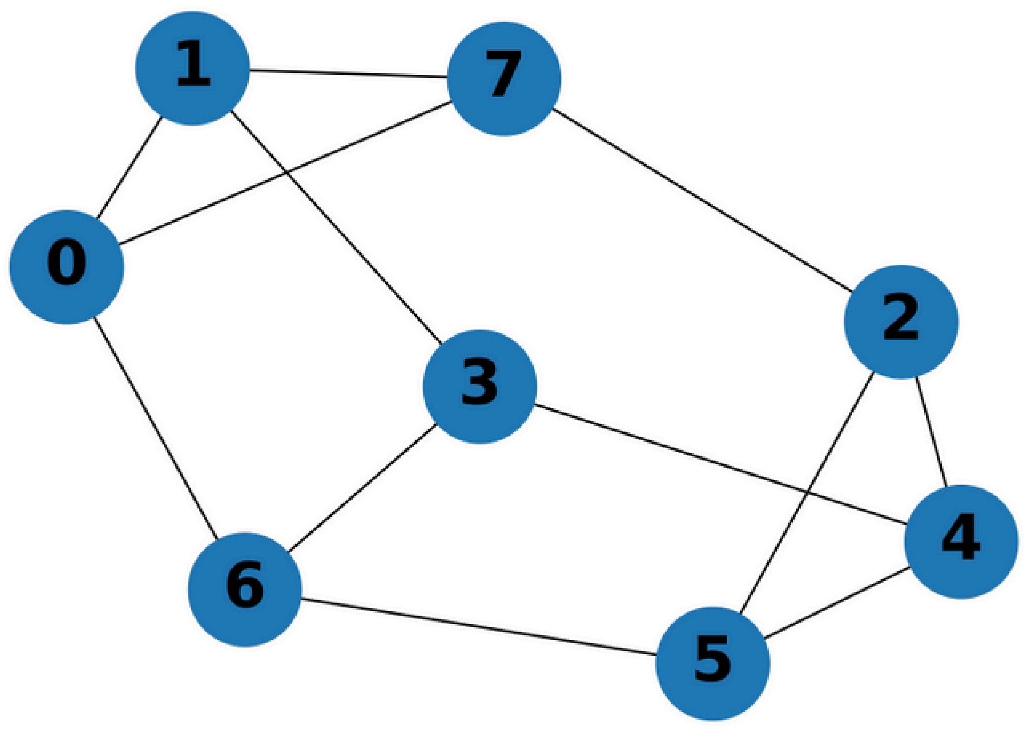
$$RY = \begin{bmatrix} cos(\frac{\theta}{2}) & -sin(\frac{\theta}{2}) \\ sin(\frac{\theta}{2}) & cos(\frac{\theta}{2}) \end{bmatrix}$$

[5] A Variational Quantum Attack for AES-like Symmetric Cryptography. ZeGuo Wang, ShiJie Wei, Gui-Lu Long & Lajos Hanzo.

Cost Function

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

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



3-regular graph

[5] A Variational Quantum Attack for AES-like Symmetric Cryptography. ZeGuo Wang, ShiJie Wei, Gui-Lu Long & Lajos Hanzo.

VQAA Circuit

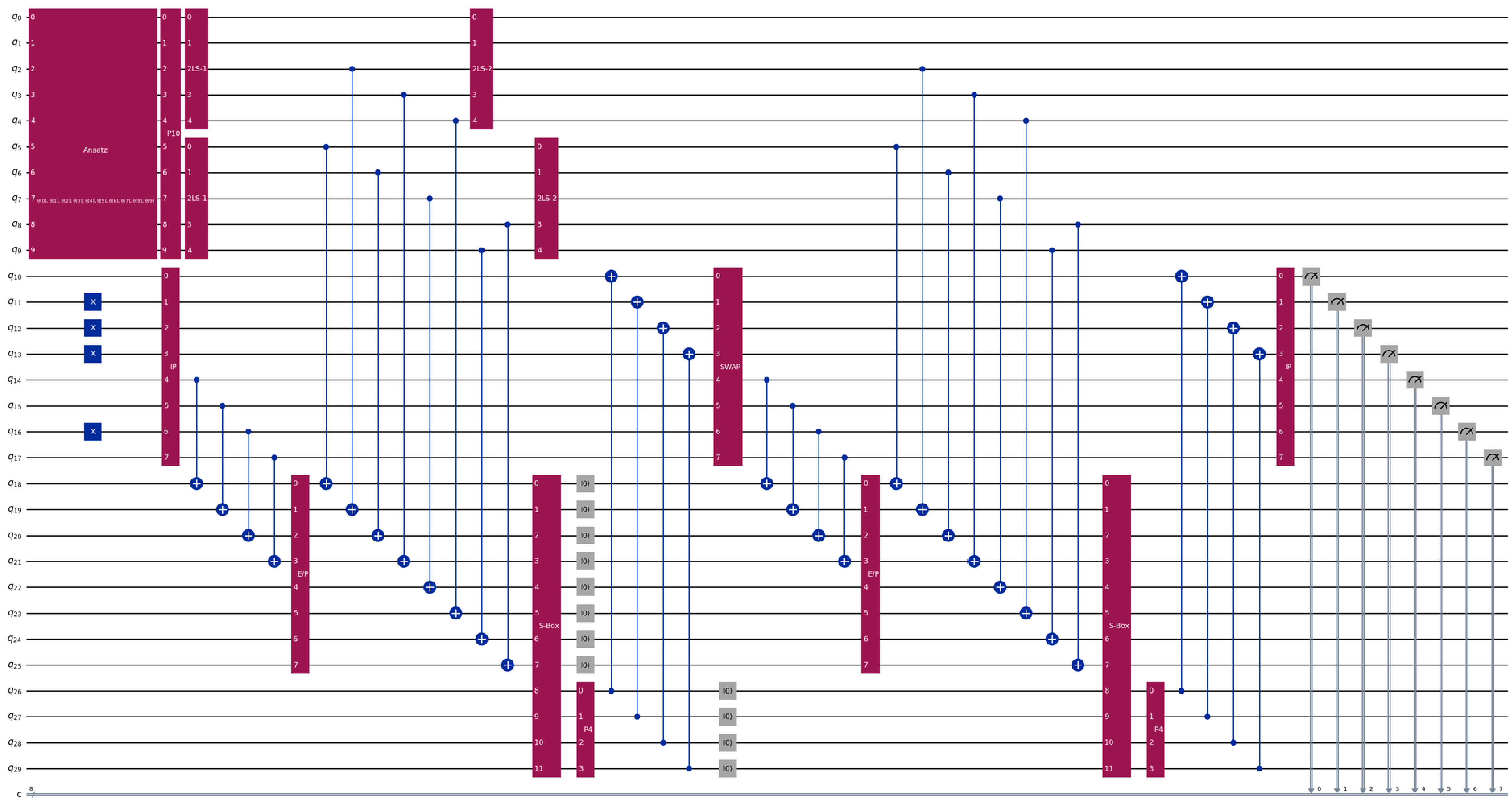


fig: VQAA Circuit

VQAA Runtime & Results

- The 30-qubit VQAA circuit was executed on IBM Sherbrooke, a 127-qubit superconducting backend.
- Due to hardware constraints, the circuit could only be run once (1 shot).
- There was too much delay in between shots causing the backend to disconnect.
- The Hamiltonian landscape observed was highly noisy and rugged, making optimization difficult.
- Overall, the results obtained were not satisfactory, and the optimization did not converge to a meaningful solution.

Issues Faced

- High Qubit Count Limits Simulation
- The choice of Ansatz & Initial parameter selection
- Extending to other algorithms is not so easy and you need to create a quantum circuit for the algorithm

Solution?

- Improved VQAA

Do we need quantum?

Yep

Do we need quantum?

- The most efficient quantum simulator - Tensor Network method, was not able to run this algorithm efficiently. Bond order was very high.
- So quantum hardware is required. Can not turn this into a quantum-inspired classical algorithm

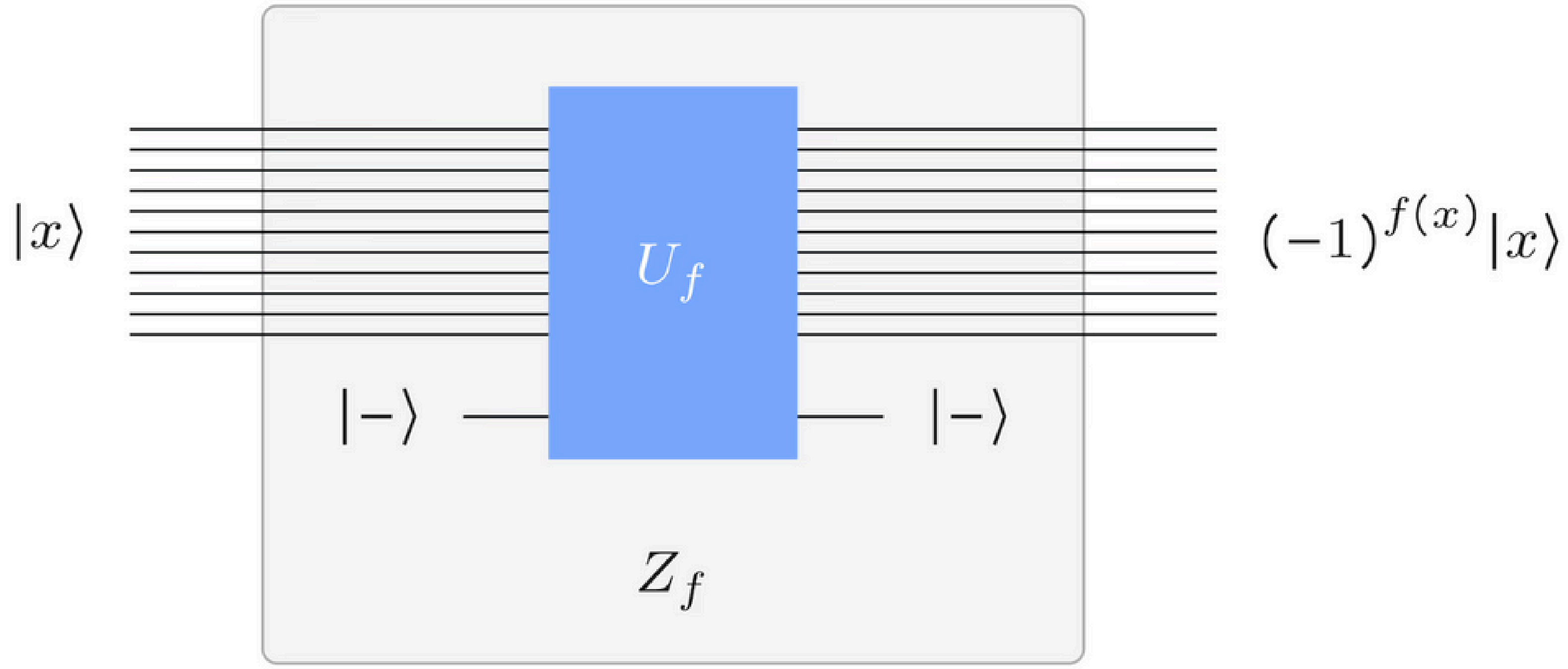
[6] Quantum Fourier Transform Has Small Entanglement. PRX Quantum, 2023.

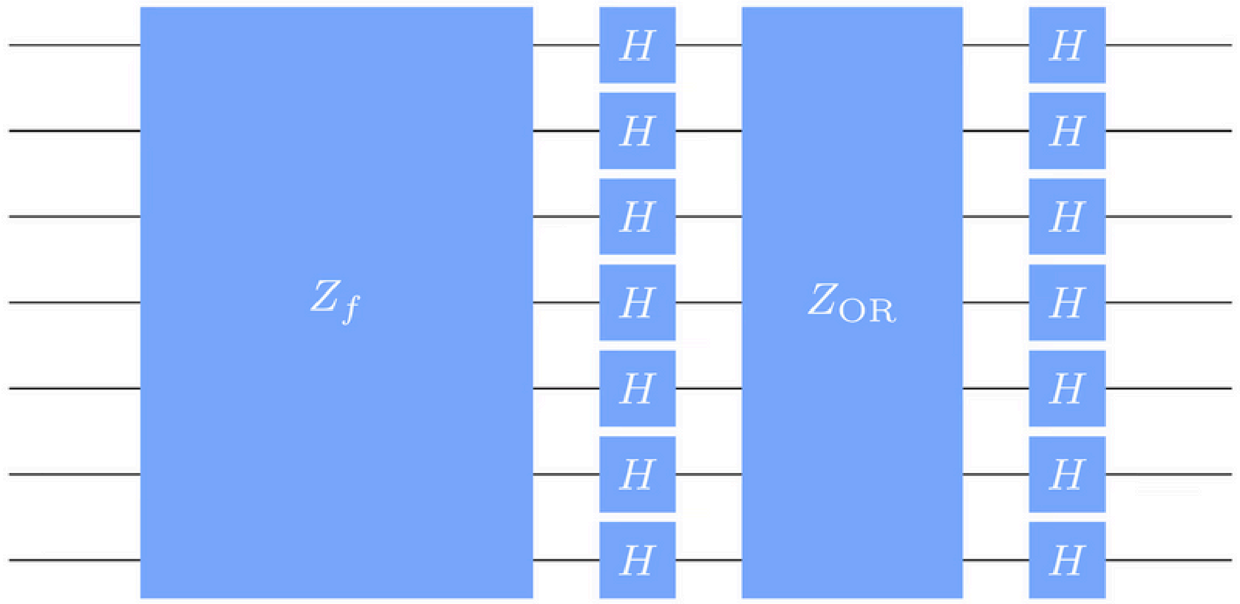
Grover's Algorithm

Input: $f : \Sigma^n \rightarrow \Sigma$

Output: a string $x \in \Sigma^n$ satisfying $f(x) = 1$, or "no solution" if no such strings exist

$$G = H^{\otimes n} Z_{\mathrm{OR}} H^{\otimes n} Z_f$$





One iteration of the grovers operator

[7] Grover's Algorithm. IBM Quantum Learning, Fundamentals of Quantum Algorithms course module.

Grover's Algorithm

$$A_0 = \{x \in \Sigma^n : f(x) = 0\}$$
$$A_1 = \{x \in \Sigma^n : f(x) = 1\}$$

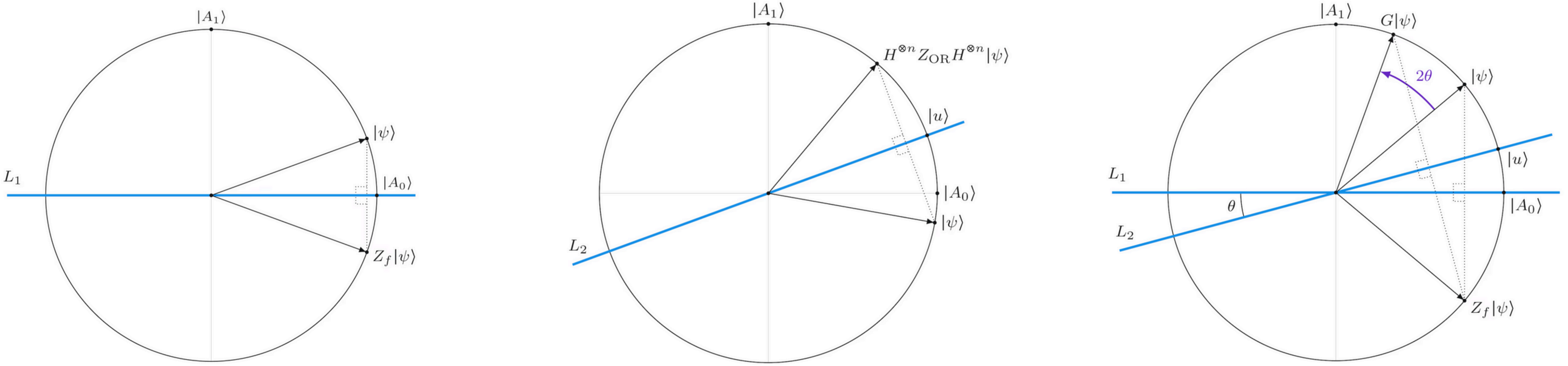
$$|A_0\rangle = \frac{1}{\sqrt{|A_0|}} \sum_{x \in A_0} |x\rangle$$
$$|A_1\rangle = \frac{1}{\sqrt{|A_1|}} \sum_{x \in A_1} |x\rangle$$

$$\theta = \sin^{-1}\left(\sqrt{\frac{|A_1|}{N}}\right)$$

$$Z_f|A_0\rangle = |A_0\rangle$$
$$Z_f|A_1\rangle = -|A_1\rangle$$

$$|u\rangle = \sqrt{\frac{|A_0|}{N}}|A_0\rangle + \sqrt{\frac{|A_1|}{N}}|A_1\rangle.$$

$$H^{\otimes n} Z_{\mathrm{OR}} H^{\otimes n} = 2|u\rangle\langle u| - \mathbb{I}.$$



[7] Grover's Algorithm. IBM Quantum Learning, Fundamentals of Quantum Algorithms course module.

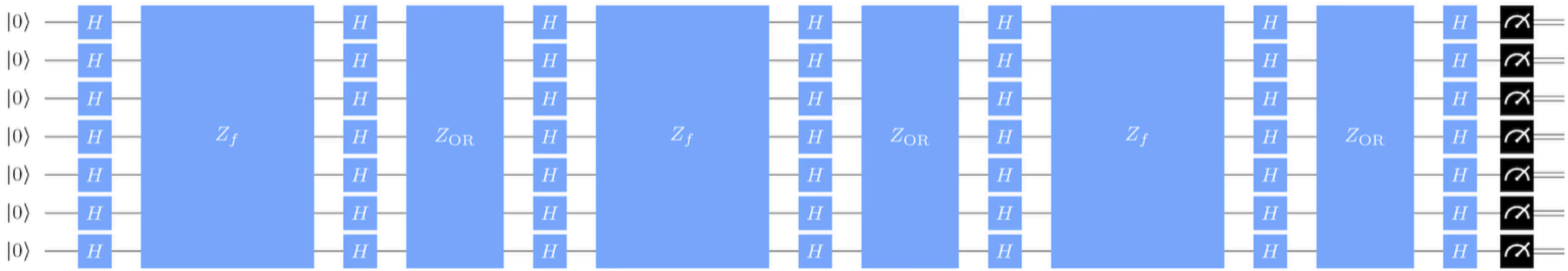
Grover's Algorithm

$$G|u\rangle = \cos(3\theta)|A_0\rangle + \sin(3\theta)|A_1\rangle$$
$$G^2|u\rangle = \cos(5\theta)|A_0\rangle + \sin(5\theta)|A_1\rangle$$
$$G^3|u\rangle = \cos(7\theta)|A_0\rangle + \sin(7\theta)|A_1\rangle$$

$$G^t|u\rangle = \cos\big((2t+1)\theta\big)|A_0\rangle + \sin\big((2t+1)\theta\big)|A_1\rangle.$$

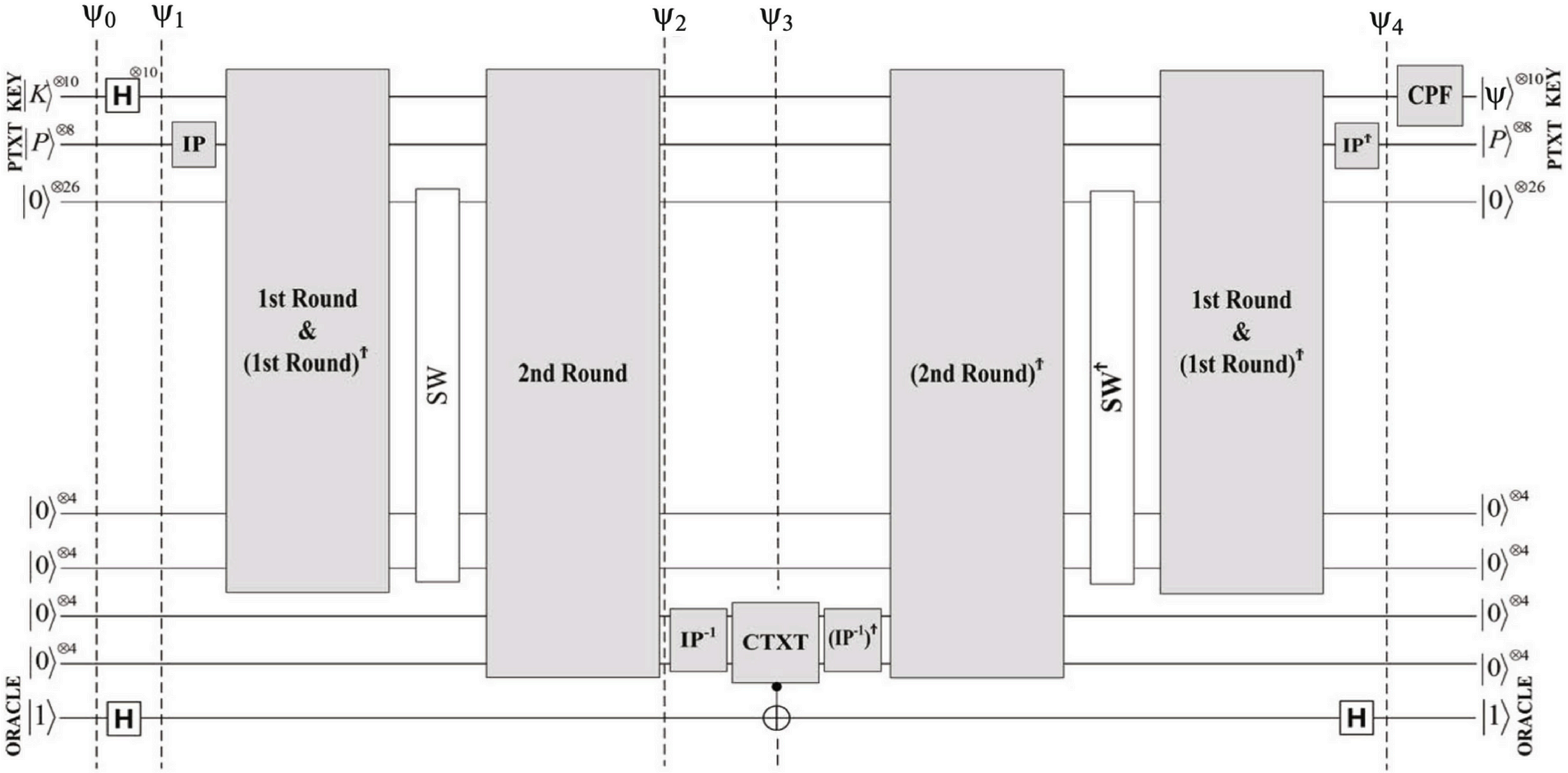
$$\theta = \sin^{-1}\left(\sqrt{\frac{|A_1|}{N}}\right)$$

$$t \approx \frac{\pi}{4\theta} - \frac{1}{2}.$$



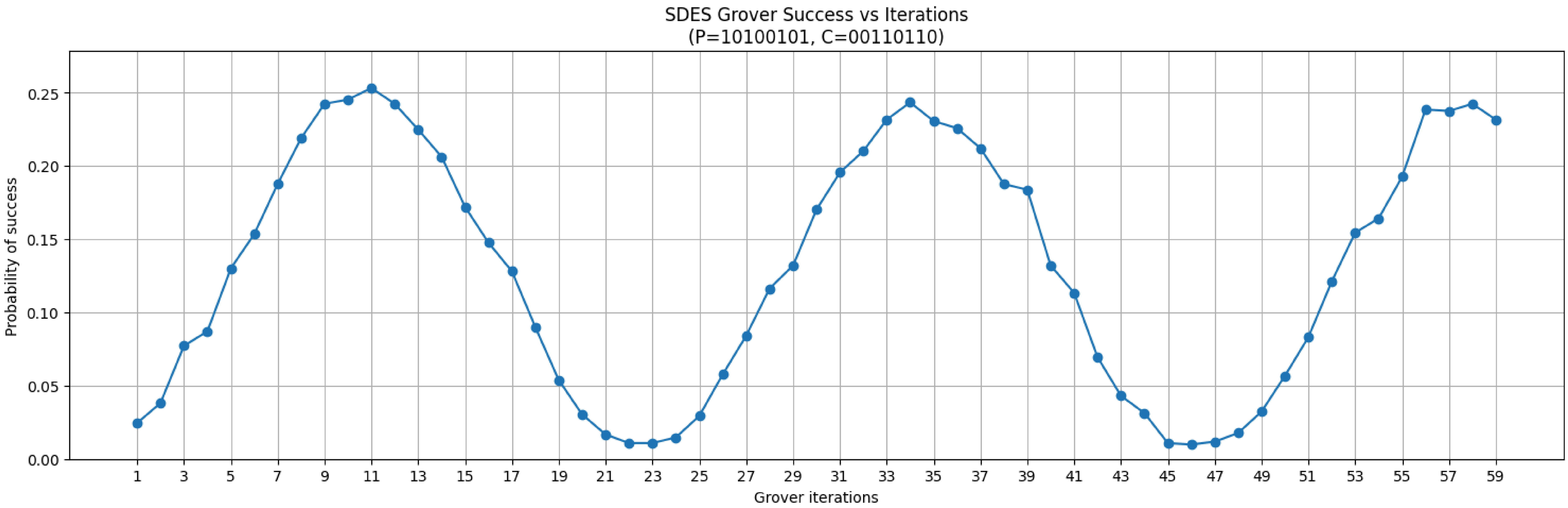
[7] Grover's Algorithm. IBM Quantum Learning, Fundamentals of Quantum Algorithms course module.

Grover's Algorithm



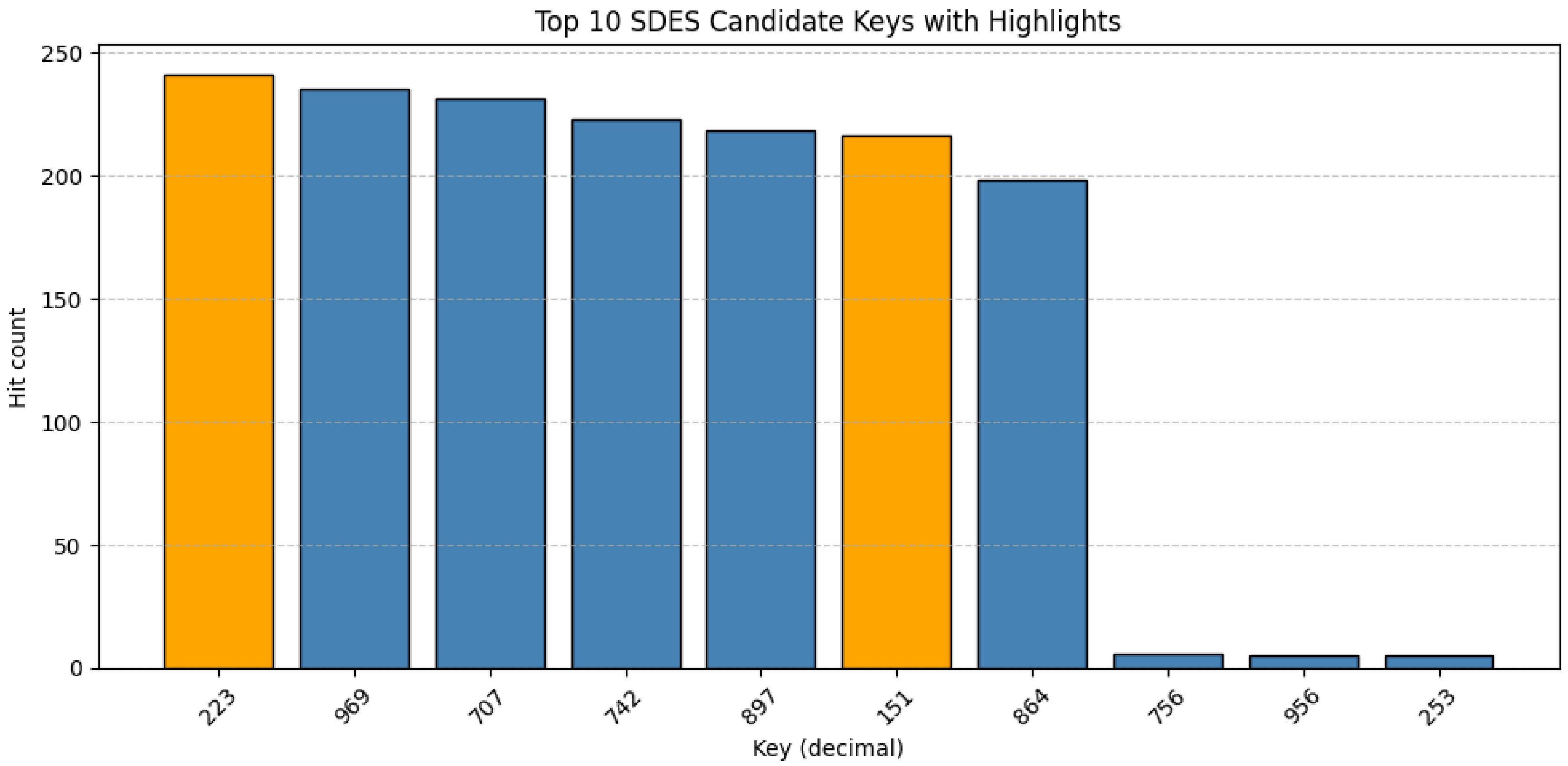
[8] Denisenko, D. V. & Nikitenkova, M. V. "Application of Grover's Quantum Algorithm for SDES Key Searching." Journal of Experimental and Theoretical Physics 128(1)

Results

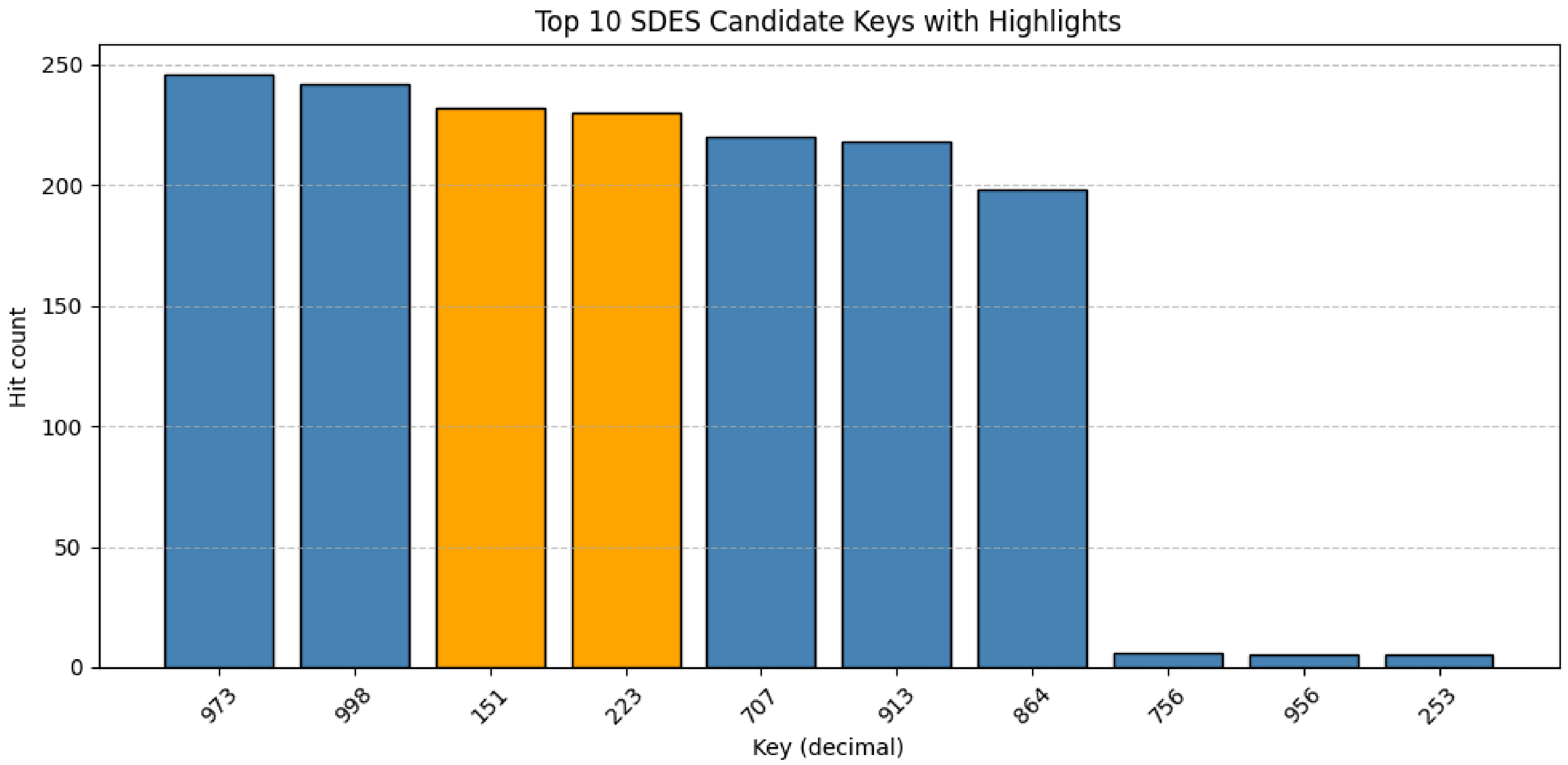


SDES Grover Success vs Iterations
(P=10100101, C=00110110)
Probability of success
0.00
0.05
0.10
0.15
0.20
0.25
Grover iterations
1
3
5
7
9
11
13
15
17
19
21
23
25
27
29
31
33
35
37
39
41
43
45
47
49
51
53
55
57
59

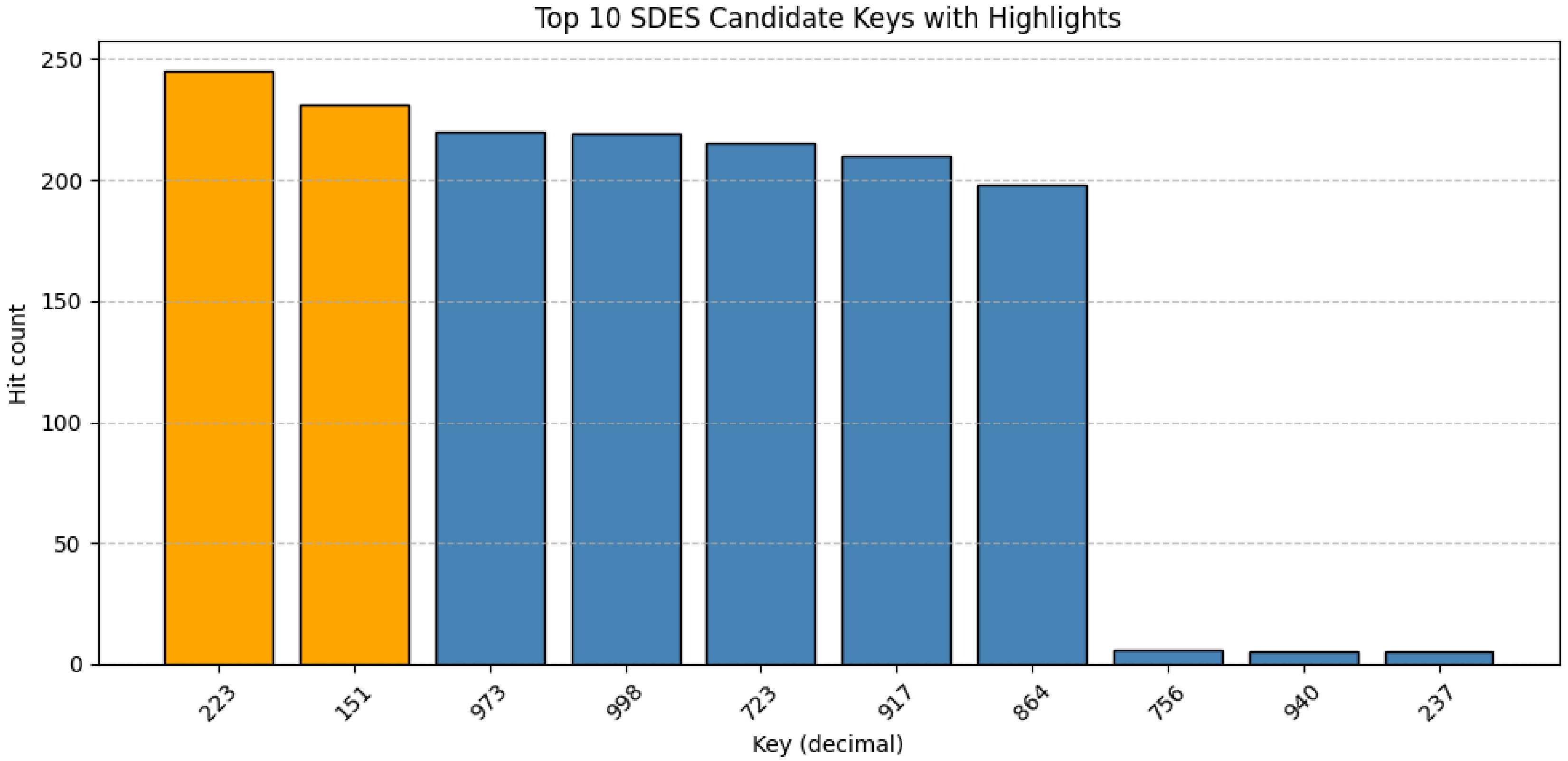
Results



Top 10 SDES Candidate Keys with Highlights
Hit count
Key (decimal)
0
50
100
150
200
250
223
969
707
742
897
151
864
756
956
253



Top 10 SDES Candidate Keys with Highlights
Hit count
Key (decimal)
0
50
100
150
200
250
973
998
151
223
707
913
864
756
956
253

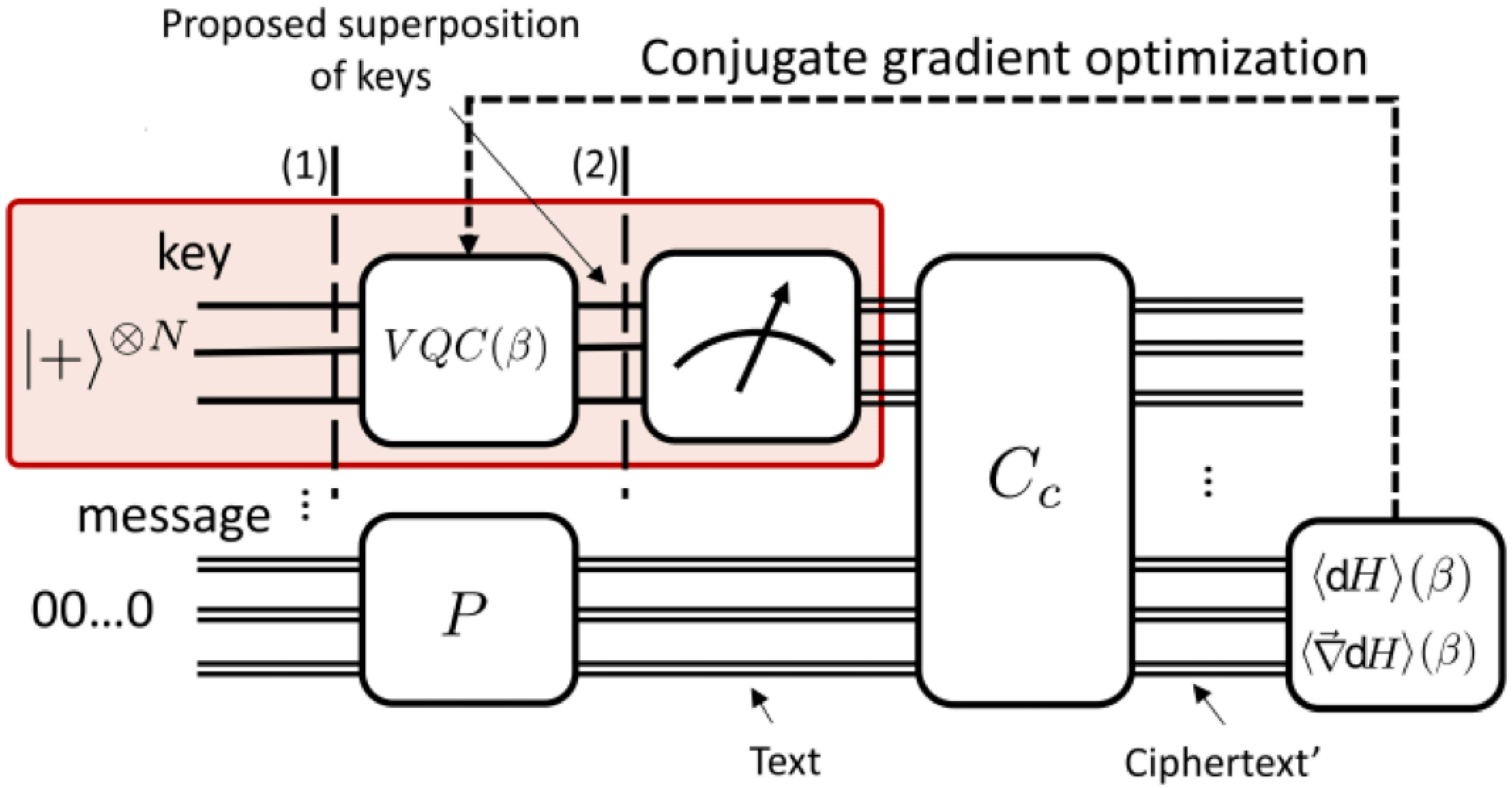


Top 10 SDES Candidate Keys with Highlights
Hit count
Key (decimal)
0
50
100
150
200
250
223
151
973
998
723
917
864
756
940
237

Interpretation

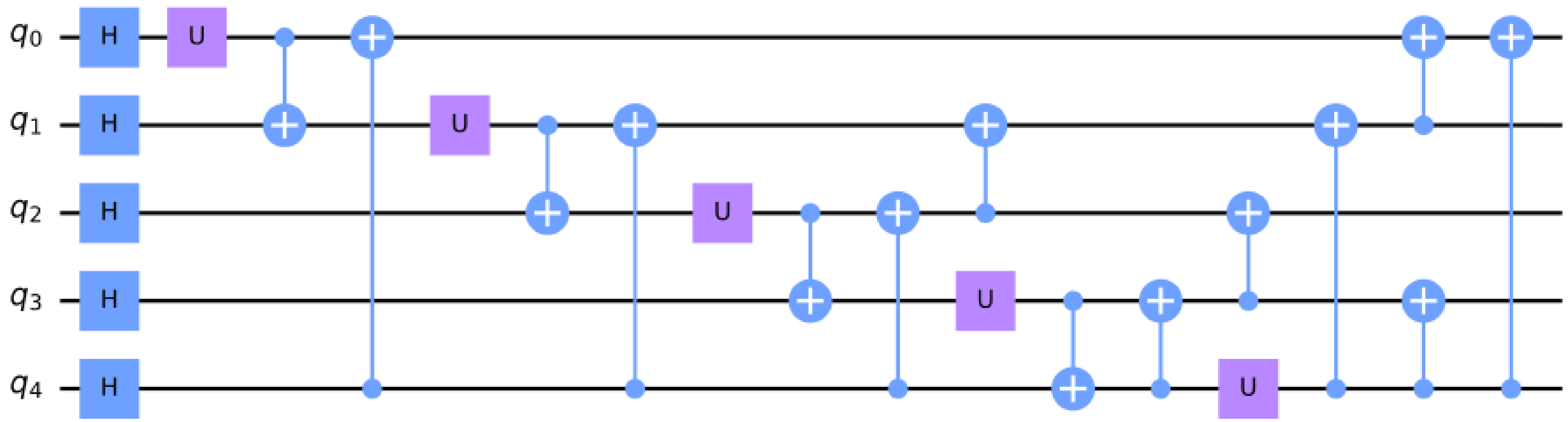
- The circuit depth is very high => Very prone to errors
- The runtime is faster than variational algorithms plus the results are more promising. Given that we have efficient hardware, this method might be very good.
- Extending to more complex algorithms is not quite that straightforward. A quantum circuit is required and for larger keys, this might not be feasible after a point

Improved VQAA



[9] Aizpurua, B., Bermejo, P., Etxezarreta Martínez, J. & Orús, R. "Hacking Cryptographic Protocols with Advanced Variational Quantum Attacks."

Ansatz Used:



$$U(\theta, \varphi, \lambda) = \begin{pmatrix} \cos\frac{\theta}{2} & -e^{i\lambda}\sin\frac{\theta}{2} \\ e^{i\varphi}\sin\frac{\theta}{2} & e^{i(\varphi+\lambda)}\cos\frac{\theta}{2} \end{pmatrix}$$

[9] Aizpurua, B., Bermejo, P., Etxezarreta Martínez, J. & Orús, R. "Hacking Cryptographic Protocols with Advanced Variational Quantum Attacks."

Results

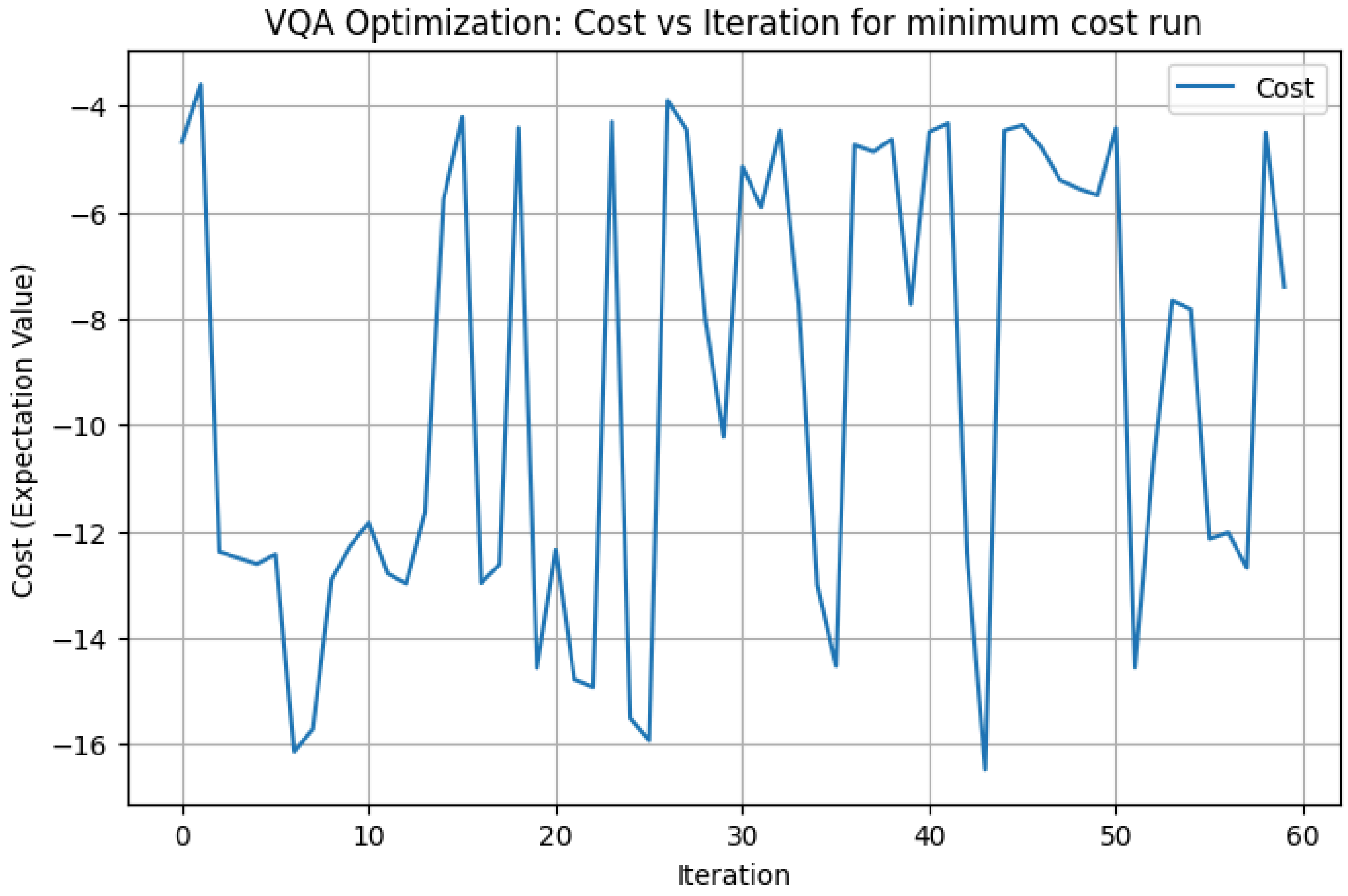
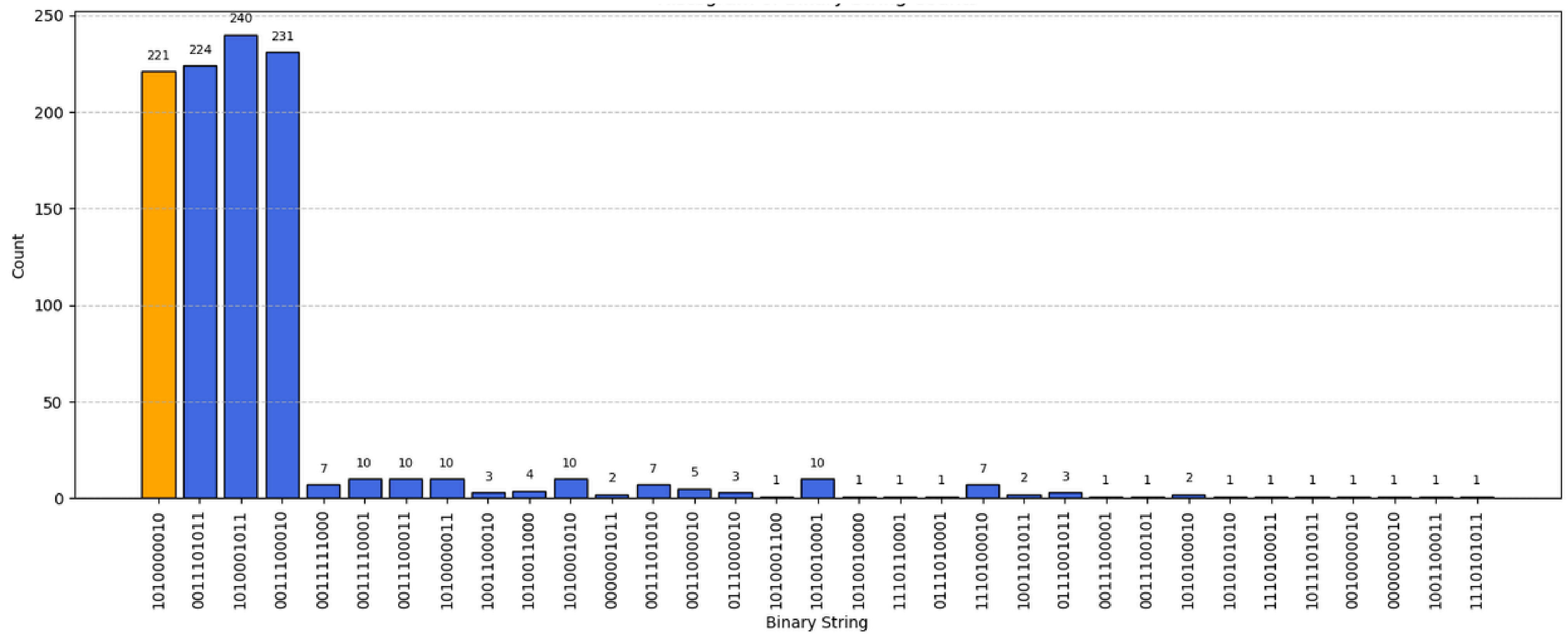


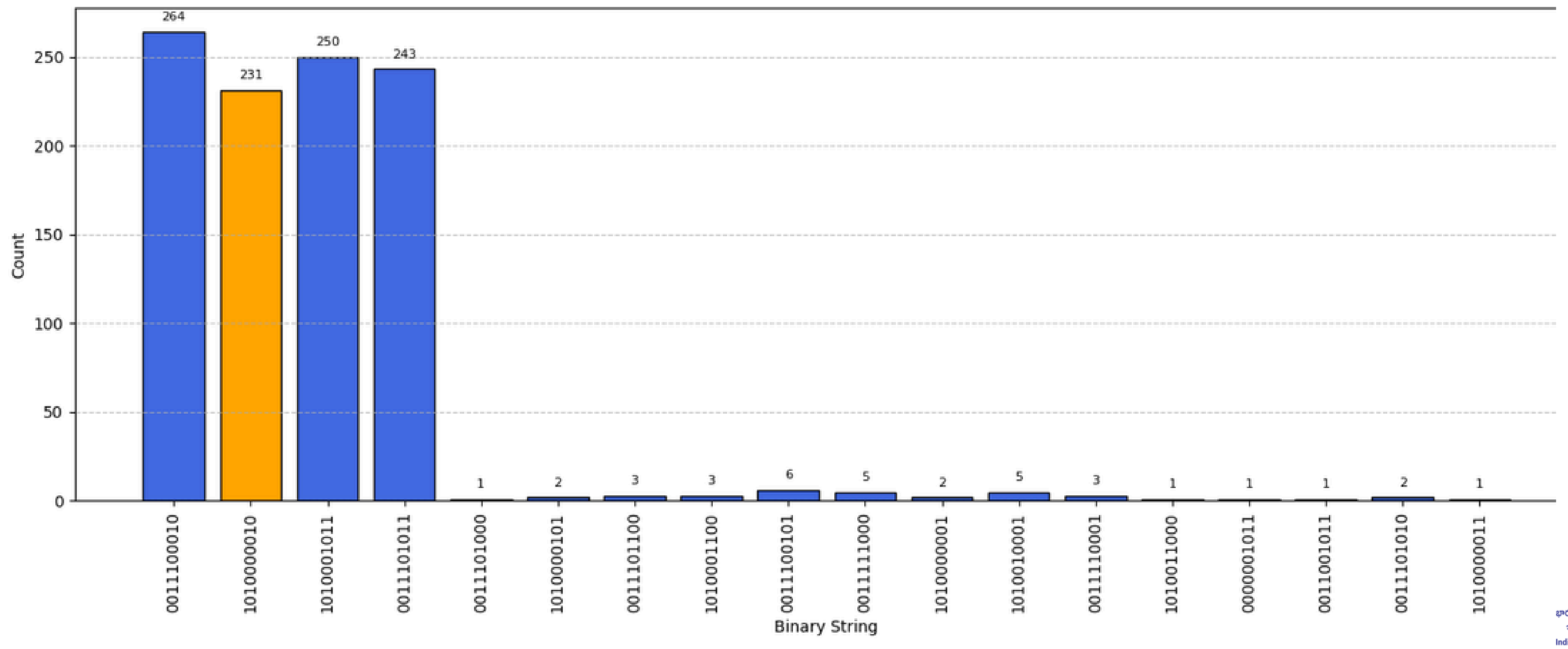
Fig: Improved VQAA cost function convergence for best params

- For a plaintext (10010111) and ciphertext (00111000), the correct key was 1010000010, which was retrieved by the Improved VQAA, was within the top 4 outputs.
- 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 ($\| \nabla E \| <$ 10−6), optimization avoided barren plateaus and converged reliably.

Results



Count
0
50
100
150
200
250
221
224
240
231
7
10
10
10
3
4
10
2
7
5
3
1
10
1
1
1
7
2
3
1
1
2
1
1
1
1
1
1
1
1010000010
0011101011
1010001011
0011100010
0011111000
0011110001
0011100011
1010000011
1001100010
1010011000
1010001010
0000001011
0011101010
0011000010
0111000010
1010001100
1010010001
1010010000
1110110001
0111010001
1110100010
1001101011
0111001011
0011100001
0011100101
1010100010
1010101010
1110100011
1011101011
0010000010
0000000010
1001100011
1110101011
Binary String



Count
0
50
100
150
200
250
264
231
250
243
1
2
3
3
6
5
2
5
3
1
1
1
2
1
0011100010
1010000010
1010001011
0011101011
0011101000
1010000101
0011101100
1010001100
0011100101
0011111000
1010000001
1010010001
0011110001
1010011000
0000001011
0011001011
0011101010
1010000011
Binary String

References

- Biryukov, A., & Shamir, A. (2002). Cryptanalysis of S-DES. Cryptology ePrint Archive
- The complexity of NISQ. Nature Communications, 2023. Nature Communications
- The Variational Quantum Eigensolver: a review of methods and best practices. arXiv preprint arXiv:2108.03993, 2021. arXiv
- The Quantum Approximate Optimization Algorithm and the Sherrington–Kirkpatrick Model. Quantum, 2022. Quantum Journal
- A Variational Quantum Attack for AES-like Symmetric Cryptography. ZeGuo Wang, ShiJie Wei, Gui-Lu Long & Lajos Hanzo.
- Quantum Fourier Transform Has Small Entanglement. PRX Quantum, 2023.
- Grover's Algorithm. IBM Quantum Learning, Fundamentals of Quantum Algorithms course module.
- Denisenko, D. V. & Nikitenkova, M. V. "Application of Grover's Quantum Algorithm for SDES Key Searching." Journal of Experimental and Theoretical Physics 128(1)
- Aizpurua, B., Bermejo, P., Etxezarreta Martínez, J. & Orús, R. "Hacking Cryptographic Protocols with Advanced Variational Quantum Attacks."

THANK YOU