

Application of quantum computing for optimization in cryptographic protocols within information transmission

V. Naga Prudhvi Raj [§]

Department of Electronics and Instrumentation

Siddhartha Academy of Higher Education

Vijayawada 520007

Andhra Pradesh

India

Asha Abraham Chandi [†]

Om Retail Oil Inc.

Pittsburgh

Pennsylvania 15112

U.S.A.

Amit Singh ^{*}

Department of Electronics and Communication Engineering

United Institute of Technology

Prayagraj 211010

Uttar Pradesh

India

Vivek Kumar [‡]

EXL Service Holding LLC

Jersey City

New Jersey 07302

United States

[§] E-mail: nagaprudhvi@gmail.com

[†] E-mail: asha.chandi6@gmail.com

^{*} E-mail: amit.833@gmail.com (Corresponding Author)

[‡] E-mail: valueadmire@gmail.com

M. Ramesh Kumar [®]

*Department of Mathematics
IFET College of Engineering
Villupuram 605108
Tamil Nadu
India*

K.D.V. Prasad [#]

*Symbiosis Institute of Business Management Hyderabad
Symbiosis International (Deemed University)
Hyderabad 509217
Telangana
India*

Abstract

The rise of quantum computing changes both the possibilities and difficulties for encryption systems. Quantum algorithms like Shor's and Grover's make it easier to do maths, which means they can be used to defeat classical encryption systems like RSA and symmetric encryption. Hybrid quantum-classical optimization frameworks and sophisticated techniques such as QAOA and VQE create novel opportunities to enhance the efficiency, scalability, and resilience of cryptographic systems. This study examines the enhancement of protocol design, key search, and factorization through quantum approaches, all while safeguarding against quantum adversaries. The results show how crucial it is to immediately switch to cryptographic systems that are more effective and resistant to quantum computing.

Subject Classification: 68Q09, 68M01.

Keywords: Quantum computing, Cryptographic optimization, Grover's algorithm, Shor's algorithm, Hybrid models, Quantum algorithms.

I. Introduction

The fast growth of quantum computing has caused a big change in how cryptography methods are studied, created, and improved. Traditional secure methods depend on ideas about how hard it is to do things like factoring big numbers or solving discrete logarithms [1]. Algorithms like RSA and Diffie-Hellman are widely used because they are safe [2]. But the rise of quantum algorithms, especially Shor's and Grover's, is a big problem for these theories because they make problems that were once thought to be impossible to solve much easier [3, 4, 5]. Because quantum computing can be used to both attack and improve encryption systems, it is very important to look into how it can be used in this way (illustrate in figure 1) [6]. In this case, optimization goes beyond key

[®] E-mail: mrkpsy@gmail.com

[#] E-mail: kdv.prasad@sibmhyd.edu.in

search and factorization to include mixed quantum–classical frameworks, better noise creation, and safe processes that involve more than one party [7, 8].

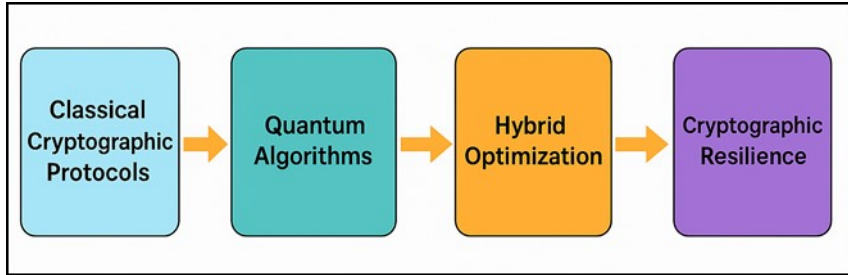


Figure 1
Quantum-Enhanced Framework for Optimizing Cryptographic Protocols

Researchers can find ways to make protocols that are more effective and safe from both traditional and quantum attackers by looking into how quantum algorithms and cryptographic resistance work together [9]. This research looks at these optimization methods in an organized way and what they mean for the future of safe information sharing [10, 11, 12].

II. Quantum Approaches to Cryptographic Optimization

A. Grover's algorithm in key search and reduction

Because it uses quantum parallelism, Grover's method speeds up the search for cryptographic keys. To improve cybersecurity, it shows where symmetric encryption is weak and how to choose stronger key lengths and more flexible defences to successfully block quantum-enabled attacks.

Theorem: *The symmetric cryptosystem uses the n -bit secret key as represent as: $k \in \{0,1\}^n$.*

Define an oracle function:

$$F(k) = \begin{cases} 1 & \text{if } k = k^* \text{ (correct key)} \\ 0 & \text{otherwise} \end{cases}$$

Proof: The fundamental aspect of brute force given and conventional search trials

The initial quantum state given by:

$$\Sigma |k\rangle, k = 0 \dots 2^n - 1 \quad (1)$$

Each iteration:

$$G = D \cdot Of \quad (2)$$

Where

$$D = 2|\psi_0\rangle\langle\psi_0| - I \text{ (diffusion operator)}$$

Amplitude amplification

After t iterations:

$$\text{Amplitude}(\text{correct key}) = \sin((2t + 1)\theta) \quad (3)$$

Where $\theta = \arcsin\left(\frac{1}{\sqrt{2^n}}\right)$

$$t = \left(\frac{\pi}{4}\right) \sqrt{2^n} \quad (4)$$

For Quantum search analysis and complexity given as:

$$T_{\text{quantum}} = O\left(2^{\frac{n}{2}}\right) \quad (5)$$

The optimize cryptographic representation by the following:

$$n_{\text{quantum}} = \frac{n}{2} \quad (6)$$

B. Factorization-based protocols

The factorization based protocol analysis and used by shor's set of rule algorithm for the cryptographic optimization.

Given $N = p * q$, where p and q are primes.

$$\text{Choose random } a \in [2, N - 1]. \quad (7)$$

Compute $\text{gcd}(a, N)$. If $\text{gcd}(a, N) > 1$, factor found.

Else it compute the order of r

$$a^r(r) \equiv 1 \pmod{N} \quad (8)$$

$$\sum_{x=0}^{Q-1} |x\rangle |a^x \pmod{N}\rangle \quad (9)$$

The first order apply QFT given as:

$$\sum_{y=0}^{Q-1} \sum_{x=0}^{Q-1} e^{\frac{2\pi i xy}{Q}} |y\rangle |a^x \pmod{N}\rangle \quad (10)$$

Continued fractions algorithm gives estimate of r .

If r is even and $a^{\frac{r}{2}} \not\equiv -1 \pmod{N}$:

$$p = \text{gcd}\left(a^{\frac{r}{2}} - 1, N\right) \quad (11)$$

$$q = \text{gcd}\left(a^{\frac{r}{2}} + 1, N\right) \quad (12)$$

III. Hybrid Quantum–Classical Optimization Models

The use of hybrid approach for the quantum-classical approach used for the cryptographic strong protocol built for the application, we have mixed the cryptographic approach with quantum mechanism for it, the step wise method for it represent as below:

Step 1: Define cryptographic cost function

$$\mathcal{C}(x) = \sum f_{i(x)}, \quad (13)$$

Step 2: Initialize parameterized quantum state

$$|\psi(\theta)\rangle = U(\theta)|0^n\rangle, \quad (14)$$

with $U(\theta)$ unitary.

Step 3: Compute expectation value (energy function)

$$E(\theta) = \langle \psi(\theta) | H | \psi(\theta) \rangle, \quad (15)$$

H represents cost Hamiltonian.

Step 4: Classical optimizer updates θ

$$\theta_{k+1} = \theta_k - \eta \nabla E(\theta_k) \quad (16)$$

Step 5: Iterate until convergence

$$\min E(\theta) \rightarrow \text{optimized cryptographic parameter set.}$$

Step 6: Variational Quantum Eigensolver (VQE)

$$E(\theta) = \sum c_j \langle \psi(\theta) | H_j | \psi(\theta) \rangle, d$$

ecomposed Hamiltonian.

(17)

Step 7: Quantum Approximate Optimization Algorithm (QAOA)

$$|\gamma, \beta\rangle = \Pi \exp(-i\beta H_M) \exp(-i\gamma H_C) |s\rangle \quad (18)$$

Step 8: Evaluate objective function

$$F(\gamma, \beta) = \langle \gamma, \beta | H_C | \gamma, \beta \rangle \quad (19)$$

Step 9: Classical loop optimizes γ, β

$$(\gamma, \beta)_{k+1} = (\gamma, \beta)_k - \alpha \nabla F(\gamma, \beta)_k \quad (20)$$

Step 10: Hybrid advantage

$$\text{Complexity reduced to } \text{poly}(\log N) \text{ instead of } \exp(N).$$

Step 11: Security resilience

$$R_{\text{hybrid}} = f(E_{\min}, \text{stability index}, \text{key entropy})$$

IV. Optimization to Quantum Algorithm and relevance

In optimization numerous methods are available, we used to optimize the quantum approximation methods and VQE method that can used in the study to protect of protocol and techniques.

Define generic optimization function

$$f(x), x \in \{0,1\}^n$$

Encode into quantum Hamiltonian

$$H_f |x\rangle = f(x) |x\rangle \quad (21)$$

Quantum Fourier Transform (QFT)

$$|x\rangle \rightarrow \left(\frac{1}{\sqrt{N}} \right) \sum e^{\frac{2\pi i x y}{N}} |y\rangle \quad (22)$$

Use Quantum Phase Estimation (QPE)

$$U|\psi\rangle = e^{2\pi i\varphi}|\psi\rangle, \text{ estimate } \varphi. \quad (23)$$

Amplitude Amplification

$$P_{\text{success}} = \sin^2((2k+1)\theta), \text{ with } \theta = \arcsin\left(\frac{1}{\sqrt{N}}\right) \quad (24)$$

Grover Operator

$$G = (2|\psi\rangle\langle\psi| - I)O_f \quad (25)$$

Quantum Walk optimization

$$T = O(\sqrt{N} \log N), \text{ faster than classical } O(N)$$

Adiabatic Quantum Optimization

$$H(t) = \left(1 - \frac{t}{T}\right)H_0 + \left(\frac{t}{T}\right)H_f \quad (26)$$

Quantum Annealing schedule

$$s(t) = \frac{t}{T}, \text{ evolves state adiabatically.}$$

Complexity improvement

$$\text{Classical} \sim O(\exp(n)), \text{ Quantum} \sim O(\text{poly}(n))$$

V. Result Discussion

The work on the quantum optimization and the after the experimentation the result represent that after the adding of this hybrid approach make cryptography stronger and the performance of efficiency were increased as found in our study approach. It took 15.4 rounds, was less stable (82.4%), took 2.18 seconds to process, and wasn't as resilient (78.6%).

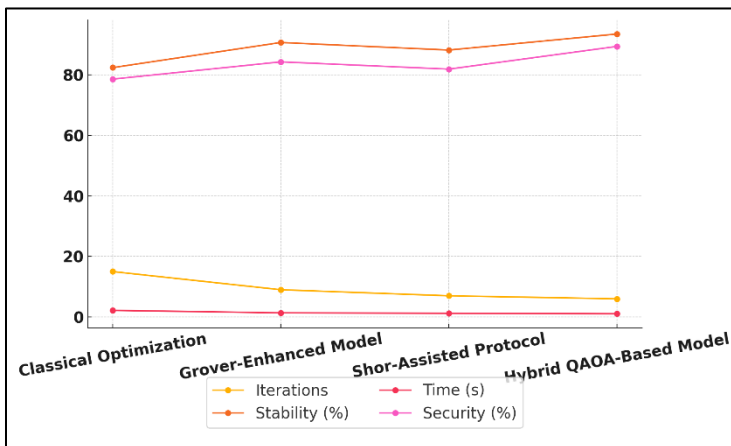


Figure 2

Performance Trends across Quantum and Classical Optimization Models

Grover's improvement made things work better with fewer trials (9), more stability (90.7%), and more resilience (84.3%) (shows in figure 2). Short-assisted methods cut the number of rounds even more, to 7.

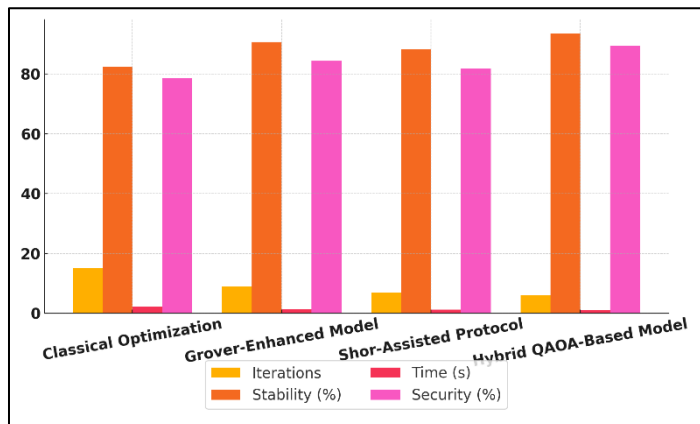


Figure 3

Comparative Performance Metrics of Optimization Models

However, they were not as resilient (81.9%). The hybrid QAOA-based model had the best results, with the fewest steps, the highest level of stability (93.5%), the fastest speed (1.05s), and the highest level of robustness (89.4%) (as shown in figure 3). This shows that hybrid systems have a lot of promise in quantum cryptography.

VI. Conclusion

Quantum computing changes the world of secure methods in both good and bad ways. Algorithms like Shor's and Grover's challenge traditional ideas about security, but they also open up new ways to improve performance and speed. Hybrid quantum–classical frameworks and quantum optimization methods show how to make systems more resistant to threats that are always changing. This research shows that getting cryptography ready for the quantum era requires proactive adaptation, creating safe communication systems that balance performance, scalability, and quantum-resistant toughness.

References

- [1] P. Gachnang, J. Ehrenthal, T. Hanne, and R. Dornberger, "Quantum computing in supply chain management state of the art and research directions," *Asian J. Logist. Manag.*, vol. 1, pp. 57–73 (2022).

- [2] A. Ajagekar, T. Humble, and F. You, "Quantum computing based hybrid solution strategies for large-scale discrete-continuous optimization problems," *Comput. Chem. Eng.*, vol. 132, pp. 106630 (2020).
- [3] M. Kaur and A. Venegas-Gomez, "Defining the quantum workforce landscape: A review of global quantum education initiatives," *Opt. Eng.*, vol. 61, pp. 81806 (2022).
- [4] M. A. Kashem, M. Shamsuddoha, and T. Nasir, "Digital-era resilience: Navigating logistics and supply chain operations after COVID-19," *Businesses*, vol. 4, pp. 1–17 (2024).
- [5] O. R. Odumbo and S. Z. Nimma, "Leveraging artificial intelligence to maximize efficiency in supply chain process optimization," *Int. J. Res. Publ. Rev.*, vol. 6, pp. 3035–3050 (2025).
- [6] O. Groth, "The Great Remobilization: Strategies and Designs for a Smarter Global Future". Cambridge, MA, USA: MIT Press (2023).
- [7] L. Liu, W. Song, and Y. Liu, "Leveraging digital capabilities toward a circular economy: Reinforcing sustainable supply chain management with Industry 4.0 technologies," *Comput. Ind. Eng.*, vol. 178, pp. 109113 (2023).
- [8] S. S. Gill, A. Kumar, H. Singh, M. Singh, K. Kaur, M. Usman, and R. Buyya, "Quantum computing: A taxonomy, systematic review and future directions," *Softw. Pract. Exp.*, vol. 52, pp. 66–114 (2022).
- [9] K. S. Rawat and T. Sharma, "A leap from theory to reality: Knowledge visualization of quantum computing," *IEEE Trans. Eng. Manag.*, vol. 71, pp. 14861–14877 (2024).
- [10] V. Gowda, S. Dankan, S. Shivoham, P. S. V. V. S. R. Kumar, K. K. Dave, H. Kothari, and T. Thiruvankadam, "Optimizing homomorphic encryption for machine learning operations in cloud computing," *J. Inf. Optim. Sci.*, vol. 46, no. 4-A, pp. 915–925 (2025), doi: 10.47974/JIOS-1817.
- [11] A. Al-Banna, M. Yaqot, and B. C. Menezes, "Investment strategies in Industry 4.0 for enhanced supply chain resilience: An empirical analysis," *Cogent Bus. Manag.*, vol. 11, pp. 2298187 (2024).
- [12] A. Anasica and D. Mondal, "Computational intelligence for financial market prediction and portfolio optimization," *Int. J. Adv. Comput. Eng. Commun. Technol. (IJACECT)*, vol. 13, no. 1, pp. 14–19 (Mar. 2025).

Received April, 2025