The Journal of High School Research

Optimizing Quantum Key Distribution Networks Using Quantum Annealing and Gate-Based Quantum Computing

Aadi Shah

Submitted: 16 October 2024 **Accepted:** 30 November 2024 **Publication date:** 07 December 2024

ISSN: 3066-2664: **DOI: 10.70671/2ft99c50**

Abstract: This paper analyzes the current Quantum Key Distribution (QKD) Model which is widely used and integrates quantum annealing and gate-based quantum computing to optimize the process. It talks about the basics of QKD, Annealing, and Gate-based quantum computing, their significance in today's world, and the existing research done on them. At the end of the paper, there is a method that proposes a new approach to integrating gate-based quantum computing and quantum annealing in QKD, which might not be feasible right now; however, when it is practically implemented, it shows how this method will be efficient, effective, and will have the least energy consumed.

Author keywords: Quantum Key Distribution; QKD; Quantum Annealing; Gate-based Quantum Computing; Qubits; Cryptography

Introduction

Background on quantum cryptography and QKD

Quantum cryptography is a paradigm shift in the way we approach cryptography in the modern world. It challenges the very foundation of classical cryptography. Quantum cryptography is built on the uncertainty principle and then built up by quantum entanglements and other properties.[1] In a world where decryption is becoming easier, we need it to help build our walls. The most well-known application of this is in Quantum Key Distribution.

Quantum key distribution is a method of encryption based on the natural laws of quantum mechanics between two people. This is a process of converting plain text into scrambled information so that only one with the right key can access it.[2] At the core of QKD, it utilizes the principles of quantum mechanics[3] to create a very secure key between the two parties. This key then encrypts and decrypts the messages, ensuring only the person with the key can access it. It plays a pivotal part by contributing to quantum cryptography.

- Unconditional Security: QKD uses quantum properties like superposition and entanglement to detect any attempt at eavesdropping. If an eavesdropper tries to intercept the key, the quantum state of the particles carrying the key is disturbed, instantly alerting the communicating parties. This is very different than classical cryptography, which focuses on mathematical difficulties that can easily be compromised[4]
- Detection of Eavesdropping: In QKD protocols, such as BB84,[2] the communication involves sending quantum bits (qubits) over a quantum channel. Any attempt to measure these qubits by a third party introduces an error in communication. Even if the receiving party tries to read these qubits, it might result in affecting the qubits, leading to an error. The security of the key is independent of the computational resources of any potential adversary, making it future-proof against the threat of quantum computers.[2]
- Secure Key Generation: QKD allows two parties to generate a shared, random secret key that is not known to any third party. This key can then be used for symmetric encryption algorithms to secure communication channels. The security of the key is independent of the computational resources of any potential adversary, making it future-proof against the threat of quantum computers.[5]

  Quantum Key distribution faces some problems in the real world

  - Operational Efficiency v/s energy consumption: The need for error correction, privacy amplification, and maintaining high secure key rates increases computational overhead and energy demand, leading to trade-offs between efficiency and energy use
  - Energy-Intensive Infrastructure: Quantum repeaters, photon sources, and detection systems, including cryogenic cooling, require substantial energy, especially when scaling QKD networks over long distances. This paper proposes how to solve the energy consumption and efficiency problems that we face during the process of QKD

*Corresponding Author: Aadi Shah. Email: jrcaadis@gmail.com
Jayshree Periwal International School, Jaipur, India

– Distance Limitations and transition loss: The photon signals weaken significantly when they travel long distances, which also leads to a lower range and also puts a halt to the range
– Side Channel Attacks: While QKD is taking place, there are a lot of vulnerabilities that occur, like information leaks or a response to light from external sources, which observers exploit

Research objectives

The objective of this research is to optimize the way we use Quantum Key Distribution based on quantum annealing. More specifically, we will be covering

1. The investigation of the potential of quantum annealing will help to enhance the efficiency, security, and scalability as it optimizes energy consumption and the response to threats
2. The mathematical algorithm will cover the integration of quantum annealing in QKD and also reduce rate errors while increasing the overall performance of the quantum communication networks
3. Feasibility and effectiveness of the integration of quantum annealing in quantum key distribution while analyzing its practical and theoretical applications
4. Identify the practical implications and challenges of implementing quantum annealing in real-world QKD systems and propose future research directions to further advance the integration of quantum annealing in quantum cryptography.

These objectives make this research a very important step towards the advancement of the future of secure communications with a focus on optimizing existing QKD technologies through the novel application of quantum annealing.

The relevance of this research

This research is vital for advancing quantum cryptography using quantum annealing to optimize Quantum Key Distribution (QKD) systems. As quantum cryptography becomes vital for the secure transfer of sensitive data, enhancing QKD efficiency and security is paramount. The study's significance lies in its potential to strengthen QKD systems by optimizing key distribution paths, reducing vulnerabilities, and slicing energy consumption through quantum annealing. This could make QKD systems more secure, energy-efficient, and scalable, paving the way for practical implementation across various real-world applications, from secure government communications to financial transactions. Moreover, this research pioneers the integration of quantum annealing with quantum cryptography, opening new avenues for exploration and setting a precedent for hybrid quantum computing methods to address complex cryptographic challenges. By future-proofing quantum security against emerging threats, this work contributes to the long-term viability of quantum cryptographic systems as quantum technologies continue to evolve. In essence, this research is a practical step towards significantly enhancing the security, efficiency, and scalability of quantum cryptography, ensuring that it remains robust and effective in a rapidly advancing technological landscape.

Introduction to quantum annealing

Quantum annealing is a quantum computational technique used to find the minimum of any given objective. They are used to solve much more complex problems. Contrary to gate-based quantum computing, which changes the state of a qubit, it goes through different gates and changes its state with every gate it goes in; quantum annealing explores the problem completely and then finds the lowest energy point.[6]

Quantum annealing suffers from problems similar to classical annealing, in which both annealing find difficulties in finding the minimum in complex and very high-dimensional places. If they go too fast, they also risk missing the minima and may settle for the local minima.[7] They also require a significant amount of resources, especially if the complexity increases. The Quantum annealer needs high coherence and low temperatures, while the classical annealer needs high-performance processing capabilities.[8] When we come down to the base of both the annealer, it depends on the way the problem is encoded and the starting conditions internally and externally.

Imagine a marble in a bowl. If you slowly tilt the bowl, the marble will continuously roll toward the lowest point, representing the ground state. If you tilt too quickly, the marble might get stuck in a higher position, analogous to the system ending up in a local rather than a global minimum. This can be compared to the working of quantum annealing where the lowest point of the bowl is the lowest energy point that this finds.

Quantum annealing is rooted in the adiabatic theorem of quantum mechanics. The central principle of quantum annealing is that the quantum systems will remain in the ground state until the Hamiltonian that describes it moves slowly.[6] The process starts with an easily preparable ground state and gradually transforms this Hamiltonian into one that covers the problem's objective function. If the transformation is slow enough, the system will end in the ground state of the final Hamiltonian; this will, in the end, be the lowest energy.[8]

$$H(t) = (1 - s(t))H_0 + s(t)H_p$$

Albash et al.[6]

H_0 = the ground state Hamiltonian

H_p = the ground state Hamiltonian

The adiabatic theorem guarantees that if the s(t) changes slowly enough, the system will remain in the ground state and will provide the optimum solution when s(t) = 1.[9]

The process of quantum annealing

The quantum annealing process starts with the **initialization**

$$H_0 = -\sum_i \sigma_x^i$$

In this scenario, where σ are the Pauli-X operators acting on the i-th qubit. This represents a superposition of

all possible states. Then, the annealing schedule governs the relation between the ground Hamiltonian and problem Hamiltonian

$$H(t) = (1 - s(t))H_0 + s(t)H_p$$

During this process, the total annealing time and the s_x and s_z are selected very carefully to ensure a smooth process. As time increases, the contribution of the H_0 decreases, and the H_p increases. This continues as it moves towards the ground state of H_p, slowly ensuring the low energy point is found.

Mathematics

The evolution of the quantum state is based on Schrodinger's equation.[9] It is governed by it and shows its evolution

$$i\hbar\frac{d}{dt}|\psi(t)\rangle = H(t)|\psi(t)\rangle$$

In the above equation, $\hbar$ is the reduced plank constant, and this equation can trace the evolution of quantum states.

Key algorithms

The proposed algorithm in quantum annealing is a hybrid quantum-classical algorithm designed for solving combinatorial optimization problems. It finds the lowest point of energy and then uses it. This structure of this algorithm starts as it encodes the problem into a Hamiltonian Hp such that its ground state is the optimum solution and takes the least amount of energy. It then uses a mixer Hamiltonian H_m [A mixer Hamiltonian is part of a system's total Hamiltonian designed to guide the evolution of a quantum state towards a desired solution state] to change and switch between states. While this process is taking place, the parameters and classical computing using the angles γ and β are taken into consideration, which optimizes the expected value of Hp.[6]

$$min(\gamma\beta)\langle\psi(\gamma,\beta)|H|\psi(\gamma,\beta)\rangle$$

Application of quantum annealing

1. The multiobjective portfolio optimization using quantum annealer
   In this study, we investigate the portfolio optimization problem using classical and quantum computing techniques, focusing on a scenario involving 'Return on Capital,' 'Concentration Risk,' and a carbon footprint constraint for 2030. The problem is reformulated as a Quadratic Unconstrained Binary Optimization (QUBO)[10] problem, and we explore its solution using quantum annealing. Although quantum annealing shows promise for addressing complex financial optimization issues, classical simulated annealing currently yields superior solutions near the Pareto frontier. This research underscores the potential of quantum computing to enhance the efficiency and robustness of financial portfolio management solutions.
2. Mapping structural topology optimization problems to quantum annealing
   This paper explores the application of quantum computing, specifically D-Wave's quantum annealing, to address complex optimization problems by converting them into quadratic unconstrained binary optimization (QUBO) models. It focuses on small-scale discrete structural topology optimization, mapping truss element variables to quantum bits, and employing a nested optimization process with dynamically adjusted cross-sectional areas. The method, validated through numerical experiments, demonstrates the potential of quantum annealing to optimize topology design efficiently despite current limitations in quantum computing resources.

Potential security vulnerabilities

Quantum systems exhibit a high degree of sensitivity to environmental factors such as temperature fluctuations and electromagnetic noise. These sensitivities can lead to computational errors, potentially undermining the security of systems that depend on quantum computing.

Quantum annealing offers promising optimization capabilities and aids in reaching the lowest energy state of a system. However, it also presents several vulnerabilities. Currently, its applications are limited, and it is not fully equipped for widespread use in practical scenarios. The extreme sensitivity of quantum systems to their surroundings poses additional challenges.

Furthermore, there are emerging attack vectors specific to quantum systems, including hacking, thermal manipulation, and strategies aimed at exploiting the annealer's control mechanisms or its environmental conditions. Additionally, quantum annealers are still in the early stages of development and lack the scalability required to effectively manage large-scale, complex security tasks, which raises potential concerns regarding the integrity of encryption and decryption processes in real-world applications.

Literature Review

Quantum key distribution (QKD) systems

The Quantum Key Distribution is a very secure way in which sensitive information is transferred using two parties to generate and share their secret keys. It depends on the fundamental laws of quantum physics and these various systems which have been mentioned below have been developed and are widely used.[4]

BB84 protocol

Developed by Charles Bennet and Gilles Brassard in 1984, this protocol is when two parties have transmitted qubits that are encoded in one of the two bases—the rectilinear and diagonal bases.[2]

The rectilinear base is a geometric design or a figure. It normally consists of straight lines and right angles, which normally make a square. However, in Quantum Key Distribution, it shows a horizontal or vertical polarized photon state at 90 degrees.

The diagonal bases are normally sets or polarization states that are oriented at 45 degrees

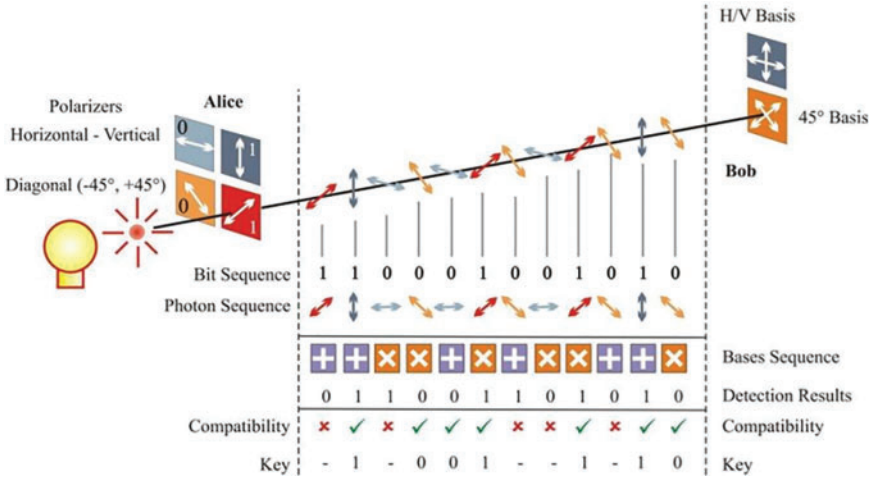

Figure 1. Illustration of Qubits Transmission between Alice and Bob (Courtesy: Stack Exchange under the license CC BY-SA 4.0 (https://crypto.stackexchange.com/questions/105609/sending-photons-in-quantum-cryptography)).

In Fig. 1, Alice and Bob randomly select their bases to measure the qubits, and after the process, they publicly compare the bases that they got and keep the bases that matched to form a key that they can use later.

To explain this better, Alice has two keys to lock a box and locks it with one of the two locks. Now she gives this to Bob, who has two keys, just like Alice. However, she does not know what will open the lock. So he tries any of the two keys, and whichever opens it is his key. This is the same way the above protocol works, but with multiple keys for the same lock, it comes together to form the actual key.[11]

While using the BB84 protocols, there is a loss of photons and a lot of noise emission when this happens. It also has finite keys to send across, which acts as a barrier to communication. When there are fluctuations, it might also cause the security of the key to decrease.

The security of the BB48 protocol is based on the no-cloning theorem and the uncertainty principle. Any eavesdropper trying to monitor them will affect their key and cause an error. There is also a QBER-Quantum Bit Error Rate in which if the error limits exceed a certain margin, the code is considered insecure, and then it is discarded.

The BB84 protocol uses basic encoding. The quantum states are encoded as $|0\rangle$ and $|1\rangle$ for the rectilinear basis and the diagonal basis; they are encoded as

$$|\pm\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

E91 protocol

The E91 protocol, created by Artur Ekert, is a quantum key distribution method that utilizes entangled photons to securely distribute keys. During the transmission of qubits, various measurements are made that aid in identifying the different quantum states.[12]

Quantum entanglement: Quantum entanglement is the phenomenon in which two particles are connected even if they are separated by a billion years. It is when a qubit is a superposition of more than one state. It is a state in which the state of one qubit is interconnected to another, and one particle instantly influences the state of the other.

This protocol is explained by the transmission between Alice and Bob in Fig. 1; in this protocol, Alice and Bob each have a pair of magically linked boxes that always have the same state. If Alice locks her box with a certain key, Bob's box will automatically lock itself with the corresponding key. When they open their boxes, the keys inside match, ensuring that no one has tampered with them. If the link breaks, then Alice and Bob's box won't open as expected.

Distributing entangled particles over a long distance is a technical issue that is not yet solved.

This protocol relies on when the Bell's inequality is not working. It is also expressed as:

$$S = |E(a,b) + E(a',b) + E(a,b') - E(a',b')| \leq 2$$

In this equation, E(a,b) is the correlation between Alice and Bob. The correlation between Alice and Bob's measurement is used to generate a key which is dependent on the rules of quantum entanglement.

Decoy state protocols

The decoy state protocols improve standard QKD methods by varying the intensity of the photon source. This variation is beneficial when an eavesdropper attempts to block certain single-photon pulses while intercepting multi-photon pulses.[5]

To clarify this, at times, Alice sends deceptive packets that resemble genuine ones but contain no real information. If an interceptor tries to access the message, they will waste time on these fake packets, allowing Alice and Bob to detect the interference.

However, this approach has a significant drawback: it increases the complexity of the process and is impacted by finite key effects, meaning that the number of keys available for use is limited.

Quantum annealing in quantum computing

Quantum annealing is a technique that is designed to find the optimum or least energy state of any function while leveraging the laws of quantum mechanics principles. It is mainly used to find the global minimum of a function from all the data, which is very large and complex. Often, it is complex and challenging but can be carried out. To make it easier to understand and find the lowest point of the valley, you will step by step go down the mountain and then find the lowest point. This is what classical devices do. In this context, the person can use quantum annealing to go to the lowest point by digging a hole through the mountain.

PRINCIPLES OF QUANTUM ANNEALING

- **Superposition:** This is a principle in quantum cryptography, which is a combination of the states 0 and 1 simultaneously. This allows the computers to work on the same problem in parallel but on different parts of the equation. It also forms distribution keys like BB84, where the superposition states are used to encode information. A qubit can be in a superposition of 0 and 1, described by a combination of amplitudes.
  Mathematically, the state of a qubit can be expressed as:

$$|\psi\rangle = a|0\rangle + \beta|0\rangle$$

  Nielsen et al.[1]
  This equation is a fundamental expression in quantum mechanics, especially in the context of quantum computing. It describes the state of a quantum bit, or qubit, which is the basic unit of quantum information. In this equation.
  $|\psi\rangle$ represents the quantum state of a qubit. It is like a vector that gives complete information about the qubit. The "ket" notation $|.\rangle$ is part of the Dirac notation, which is a standard way to denote quantum states.
  $\alpha\beta$ are complex numbers. These coefficients determine the probability of the qubit being in the $|0\rangle$ or $|1\rangle$ state.
  The probabilities of measuring the qubit in these states are given by $|\alpha|^2$ and $|\beta|^2$, with the constraint that:

$$|\alpha|^2 + |\beta|^2 = 1$$

  This property allows them to work on many parts of the equations or different things simultaneously, providing a potential for exponential speedup in solving certain types of problems.[1]
- **Quantum tunneling:** Quantum annealing is when the qubits can pass the energy barriers of going through the local minima to reach the global minimum. It should not be possible due to insufficient energy. This phenomenon is based on Schrodinger's Equation:

$$\frac{-h^2}{2m}\frac{d\psi(x)}{dx^2} + V(x)\psi(x) = E\psi(x)$$

  During the process of quantum tunneling, the wave function decays inside the barrier while it has enough energy to pass through the barrier For a potential barrier with a height h and width a. The probability of the particle passing through the tunnel is

$$T \sim e^{-2ka}, \frac{\sqrt{2m(h-E)}}{\hbar}$$

  -T represents the transmission coefficient, which gives the probability of a particle tunneling through a potential barrier in quantum mechanics; k represents the wave number inside the barrier, related to the energy of the particle and the height of the potential barrier; a represents the width of the potential barrier; m represents the mass of the particle; h represents the height of the potential barrier (also referred to as the potential energy); E represents the energy of the particle; $\hbar$ represents the reduced Planck constant, defined as $\hbar = \frac{h}{2\pi}$, where h is the Planck constant.[7]
- **Adiabatic theorem**
  The adiabatic theorem is a very important part of the quantum annealing[13] process. This ensures that the process is going slowly, which helps them find the optimum solutions and ultimately find the ground state. In the process, Hamiltonian is the total energy of the system (H(t)), which shows the energy of the system at time t

$$H(t) = (1 - s(t))H_0 + s(t)H_p$$

  In this, s is a time-dependent constant that varies from 0 to 1 as the time increases from 0 to t This theorem also states that if the process is slow enough, it will remain at its optimum state.

$$\frac{|\langle\psi(t)|\frac{dH(t)}{dt}|\psi_0(t)\rangle|}{((E_1(t) - E_0)(t))^2} \ll 1$$

  In this function
  $\psi_0\rangle$ is the ground state of the Hamiltonian H(t) at time t
  $\psi_1\rangle$ is the ground state of the Hamiltonian H(t) at time t
  E_x are the corresponding energy levels
  In the end, The Adiabatic theorem ensures that if the process is slow enough and is carried out after meeting all the requirements, it will ensure that the quantum system will stay in the lowest energy state.[6]

There have been many previous important studies related to quantum annealing in cryptography.

Evaluating Quantum Annealing for Cryptographic Applications written in 2020 was a paper based on the potential of quantum annealing in different contexts, including encryption schemes. It also discusses the current problems of the current quantum annealing for cryptographic applications.[14]

"*Quantum Annealing and Its Potential Impact on Cryptographic Security*" is a paper that explores the potential

impact of quantum annealing on existing cryptography and also reviews how it might be used to break these systems and how important it is to develop quantum resistance cryptography.[15]

Both papers talk about how quantum annealing can improve cryptography, but this paper focuses on implementing quantum annealing in QKD practically and theoretically.

Dual quantum paradigm (DQP)

The Dual Quantum Paradigm(DQP) is a process that consists of two quantum computing approaches: gate-based quantum computing and quantum annealing. This approach mentioned in the paper aims to use both strengths to solve very hard and complex problems more effectively and efficiently.

- Gate-Based Quantum Computing
  This is a method that uses gates to manipulate the qubits. There are various gates like (Pauli-Y, CNOT, etc.) which are represented by unitary matrices that act on vectors, and the state of a quantum system is represented by a vector in a Hilbert space[1].

Unitary Operators:

Unitary operators are fundamental in quantum mechanics for storing the structure and properties of quantum states. They maintain the norm of vectors, ensuring that the inner product, which represents probabilities, remains constant during quantum evolution. This assures that the total probability remains 1, crucial for the consistency of quantum theory. Unitary operators are also reversible, meaning the operation can be undone by applying the operator's Hermitian adjoint, $U^{\dagger}$ [9]. This property is essential for quantum computations, where reversibility is a key feature. Additionally, the eigenvalues of unitary operators are complex numbers with an absolute value of 1, lying on the unit circle in the complex plane. This characteristic ensures that unitary operations do not alter the magnitude of quantum state vectors, thereby preserving their length and thus maintaining the integrity of quantum information during transformations.

$$U(\theta,\phi,\lambda) = e^{ia}\begin{pmatrix} cos\left(\frac{\theta}{2}\right) & -e^{i\lambda}sin\left(\frac{\theta}{2}\right) \\ e^{i\phi}sin\left(\frac{\theta}{2}\right) & e^{1(\phi+\lambda)}cos\left(\frac{\theta}{2}\right) \end{pmatrix}$$

1. θ, ϕ, λ are real parameters that define the rotation angles.
2. e^{ia} is a global phase factor, which does not affect the probability distribution and can often be ignored in quantum computing.[9]

This is the general unitary operator for a single qubit. The parameters here can be understood as specifying rotations of qubits on the Bloch sphere [Fig. 2]. Common quantum gates like the Pauli gates X, Y, Z, the Hadamard gate H, and the phase gates S and T are all specific instances of unitary operators acting on qubits.

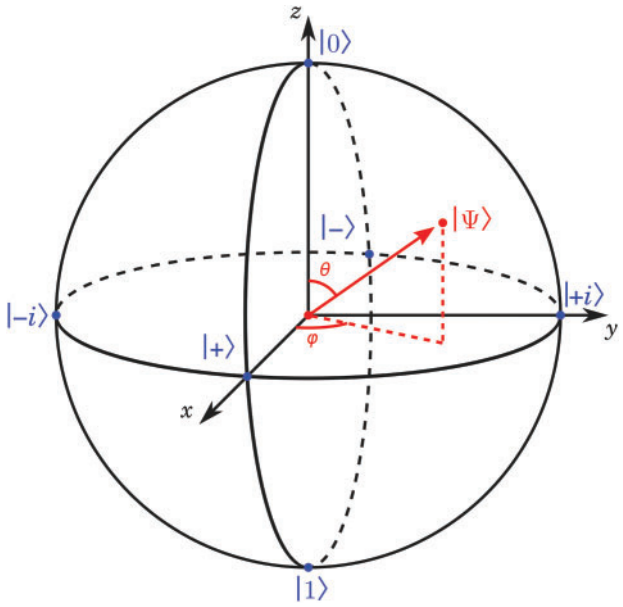

Figure 2. Bloch Sphere (https://prefetch.eu/know/concept/bloch-sphere/).

Quantum State Representation:

The state of a quantum system with n number of qubits is shown with a vector of a wave function like $|\psi\rangle$ in a 2D Hilbert's space

$$|\psi\rangle = \sum_{i=0}^{2^n-1} a_i|i\rangle$$

Here a_i is a complex co-efficient

Hamiltonian and Energy Eigenstates: The Hamiltonian is the total amount of energy that the system consists of. It also helps in determining the system's time evolution and its updates of its total energy. Meanwhile, the energy eigenstates are solutions to time-independent Schrodinger's equation.

Integrating quantum annealing in gate-based quantum computing

This combines two approaches to make this integration work. The first is gat-based quantum computing for quantum error detection and state verification, and the second approach is quantum annealing,[13] which is used to get the optimum energy state.

The Hamiltonian equation is a very important part of this integration, and it represents the total energy of a system. The main principle of the integration is the Combined Hamiltonian, which is formed with the Hamiltonian of Annealing and the Hamiltonian of Gate-based quantum computing.

$$H_{gate+annealing} = H_{gate}(t) + H_{annealing}(t)$$

The combined Hamiltonian leverages the gate-based quantum computing and quantum annealing.

At the beginning of the process, the energy associated with gate-based quantum computing is predominant as the

system performs quantum operations, specifically executing unitary transformations. As the process continues, the energy shifts toward being dominated by quantum annealing, which emphasizes optimization and reduced energy consumption. This transition can be expressed by the following equation. Throughout the process, the system's energy evolves from being primarily influenced by gate-based quantum computing to that of gate-based quantum annealing. The energy for gate-based quantum computing can be represented as follows:

$$E_{gate} = \langle (t)|H_{gate}(t)|\psi(t)\rangle$$

The energy for quantum annealing can be written as

$$E_{annealing} = \langle \psi(t)|H_{annealing}(t)|\psi(t)\rangle$$

While integrating quantum annealing in gate-based quantum computing, the prominent energy at the start is gate-based quantum computing, which takes care of the arithmetic part of the equation, and then annealing is used for using the lowest energy state. Even though this makes the process more efficient, the viability of this theory is still a question.[6]

Gaps in current research

At this time and age, Quantum annealing and cryptography have been discovered a lot theoretically, but there have been very few to test them practically instead of theoretically. Even when we talk about QKD, most of the research on QKD is done on a very small scale and not on bigger models, which fail to capture the complexity of these functions in the real world. Quantum annealing is also very sensitive to noise, making it significantly difficult when applied to QKD systems. All the materials that are present to date, like the D wave annealers, are very limited in terms of connectivity, and they reduce their ability to solve QKD problems. While carrying out research for such concepts or theories, there is a significant lack of mathematical models and benchmarks that can be used to compare the results and effectiveness of the annealing models. In addition, the QKD protocols very frequently involve continuous variables incompatible with the nature of quantum annealing. Hence, whenever they work together due to the nature of the qubits in QKD. Mainly, the security concerns of quantum annealing haven't yet been solved, which means that when we use quantum annealing in QKD, it might be exploited by future attackers.

Theoretical Framework

Quantum annealing and gate-based computing in QKD optimization

This theoretical framework is comprised of very advanced quantum computing techniques that are used to optimize the QKD and make it energy-effective. This approach projects increasing efficiency and security and scaling QKD networks as its application will help make them better. The components break down the parts of the system, making each and every part of a relic that can enhance the working of a normal QKD model. This theory is integrated with a combination of a gate-base quantum computing system and quantum annealing within a single QKD system. It uses the strengths of both theories to ensure that they are the perfect combination for this framework and that their strengths are used in the best combination. The model overall uses different Hamiltonian as it takes into consideration the different components of quantum computing paradigms that influence the working of this model.

In this model, the hybrid Hamiltonian H(t) is written as:

$$H(t) = H_{gate+annealing}(t) + H_{QKD+annealng}(t) + \lambda H_{energy}(t)$$

In this equation

$$H_{energy}(t) = \sum_i E_i x_i$$

In this equation, E_i is the energy associated with each quantum operation.

As the model starts working, it incorporates real-time adjustments to the QKD paths and the key generation parameters relying on the network conditions, ensuring the QKD system remains remarkably unaffected by environmental changes and security threats. Quantum annealing is used continuously to optimize the paths through which the keys are transmitted, reducing the factors of signal attenuation and also taking the least energy-consuming path.

Then, the system formulates the key rate, at which point we apply quantum annealing to optimize these parameters, such as signal intensity and modulation schemes, to maximize the secure key rate and minimize the error rate. When these parameters are implemented into the key generation system, they increase the security. Throughout the process, we also find out the cost function for energy consumption while taking into consideration the operational energy needs of the quantum gates and communication channels.

While quantum annealing is used to optimize the path they use, gate-based quantum computing optimizes the keys that they use, along with providing a framework for performing very detailed and controlled operations. They contribute to the Error Correction process in which they implement the error correction codes and maintain the integrity of the sensitive information. They ensure the keys are transmitted without corruption and in the most secure state. Quantum gates also enable the manipulation of quantum states with very high accuracy. It is important for initializing the qubits in the QKD system. As they contribute to the error correction, they also indirectly contribute to enhancing the stability of the model relying on the QKD model, as it is very important in practical implementations where noise also has a chance of affecting the quantum keys. Additionally, gate-based quantum computing allows the confirmation of quantum states through its gates and also verifies the model that confirms that the keys distributed by QKD are accurately transferred. Integrating this with quantum annealing reduces energy consumption, making sure that it is optimized as well as accurate. The combination of quantum annealing and gate-based quantum computing

into QKD is practically challenging but very accurate and energy-efficient.

Mathematical formulation

The QKD systems use both gate-based quantum computing and quantum annealing in which the foal is to optimize key factors like distribution paths, energy consumption, and threat response. In this, the optimization is also achieved by obtaining the Hamiltonian of quantum annealing which is also supported by gate-based quantum operations.

1. The objective of the first part is to find that is the most efficient while minimizing the cost and decreasing the noise, distance, and foreseeable attacks. This formula can also be formed as a *Quadratic Unconstrained Binary Optimization problem*, which is very suitable for quantum annealing.

    - $x_i \in \{0, 1\}$ represents whether the path i is 0 or 1
    - Q_{ij} is the cost that is caused because of the interaction of the paths i and j, which is things like noise
    - b_i is the individual cost of choosing I, this includes factors like distance and noise levels

    The Hamiltonian present here tries to minimize the cost of the path where. In this case, quantum annealing is used to minimize the Hpath for the key distribution. In the algorithm, define a cost matrix, which is Q, which shows the interaction between the two paths. It uses quantum annealing to minimize the Hamiltonian and optimize the paths.
2. The energy is also a main factor of this equation in which we seek ways to minimize the energy consumption in which multiple quantum and classical operations occur at the same time.

    The energy optimization Hamiltonian is also written as:

$$H_{energy}(x) = \sum E_i x_i$$

    Here Ei represents the energy consumption for choosing the path i. In this set of energy costs E for each path that they take.
3. In QKD, the main error that we can minimize is QBER, which is the proportion of bits that can be incorrectly sent across the users

$$QBER = \frac{N_{error}}{N_{total}}$$

    The goal is to carry out the optimization process by which the errors are decreased.
4. Quantum annealing is also used to minimize the QBER by the best settings, which involves making the signal intensity transmission rate and modulation schemes to reduce the errors in the transmission lines.

Methodology

Simulation setup

To simulate a Quantum Key Distribution (QKD) model that combines gate-based computing with quantum annealing, it's essential to establish a robust framework that effectively models these processes and allows for thorough evaluation. The use of quantum annealing simulation tools is crucial for optimizing the criteria of the QKD system, reducing errors, and identifying efficient photon travel paths. We can utilize the d-Wave Quantum Annealer, specifically designed by D-Wave Systems for tackling optimization problems while minimizing errors. This system can handle thousands of qubits to address Quadratic Unconstrained Binary Optimization (QUBO) challenges. Moreover, it is necessary to have tools that can map the Hamiltonian and energy landscape onto the qubit architecture. The system is equipped with an annealing schedule, a parameter that regulates the duration required to transition from the initial Hamiltonian to the optimized solution. For gate-based quantum computing, platforms like Qiskit and various quantum simulators can be leveraged to create comprehensive circuit designs and execute them on actual hardware. These platforms enable the implementation of algorithms such as Quantum Fourier Transform and Quantum Phase Estimation, facilitating the development of custom designs and the integration of classical computing resources when necessary.

The Quantum Network is a part of this model, which needs a lot of backend strength to handle much more complicated algorithms than it normally uses. The quantum key distribution systems in this mode need a quantum channel, classical post-processing units, and error correction algorithms. It is a good, tried, and tested choice to use the BB84 protocol combined with correction and privacy amplification. There should be a quantum source that can provide us with a source of entangled or polarized photons for key distribution and also simulate photon transmission over a fiber optic network with a changeable distance in which this is set up. It should also have quantum channels to transmit quantum states between 2 parties, as well as a noise channel that can be experimented on. Photon detectors are needed to simulate imperfections in photon detections, which also consist of dark counts and timing errors. From time to time, it can also introduce realistic errors based on actual hardware configurations. Key rates should match the real rates, making it easy for us to find the actual rates.

While integrating quantum annealing into this process, there should be initial configurations. It is very important to formulate the total error Hamiltonian that considers the noise and detects the imperfection along with extracting the optimal parameters from the annealers.

This simulation framework provides a detailed framework for evaluating the integrated QKD model that uses quantum annealing and gate-based quantum computing.

Results and Analysis

Simulation results

In this model, it is very difficult to find practical results, and it might also lead to a lot of work in the future, which may result in making this practically possible and also solving the issues that this comes with. Some of the possible and simulated outcomes for this QKD network are

1. The transmission distance of the network is very helpful in using QKD along long networks without it getting affected by other parameters. It is above the threshold which allows maintaining secure QKD through very long distances, keeping the errors to a minimum
2. Error Rate and Key Rates are optimized with quantum annealing, which helps reduce the rates of errors for a 50km fiber-optic channel. The optimization also reduces the error rate from 5 to 2 percent, showing a glimpse of quantum annealing's enhancing performance
3. Optimized circuits for gate-based computing in which the gate-based computing systems can see how they can reduce their circuit energy consumption and also increase their efficiency

These methods won't only increase their effectiveness but also show how these methods, if carried out in the real world, can be a much more desired approach as they provide the range and the efficiency that can't be found up until this date.

Practical Implications and Future Work

Implementation in real-world QKD systems

This model and theory can be the perfect key for the world of quantum computing if one has enough resources to carry it out. In today's world, this cannot be obtained due to the complexity of the criteria that are needed to complete it.

It can be used over a wide range of things in the future, for instance, it can be used for military and government communications in which they can protect sensitive communications and data transmission in military sectors. They ensure that the highest level of security is provided using this model. It can also be applied in the financial sector, where communication between banks can be more confidential and secure, and transactions can be secured with much higher data integrity than in today's world. In today's world, the model is ideal for securing patient data and records in healthcare institutions.

In today's world, everything that can be built up can be broken down, but this theory is the one that combines all the knowledge of widely used cryptography data and leverages the best to make the best and also make it so efficient that it is cost-efficient along and energy efficient There are multiple challenges that one can face while building and implementing this in real life. Integrating this model encompassed multiple challenges. The complexity of this is to a very high extent, as it consists of three different types of quantum paradigms, which require cutting-edge technology along with a perfect point at which we can find the balance of least expense and most efficiency. It can balance the rates of error rates, distribution paths, and other various factors. There are various scalability issues that can arise while integrating classical computers and quantum computers as we will need the model environment for this to work.

Ensuring security against emerging quantum threats and safeguarding data privacy are critical, requiring constant updates and advanced cryptographic techniques. Practical implementation also poses challenges, including real-world testing and ensuring interoperability with existing infrastructure. Lastly, high development costs and efficient resource management are essential considerations, requiring careful planning and potential funding strategies. Addressing these challenges involves a multidisciplinary approach and collaboration across various fields of expertise.

Conclusion

This research has a theoretical side that is much more than a practical one. It is much more theoretically based, and it cannot be implemented with the current available resources. This theory poses many things that will help make our current quantum computing methods much more efficient. With the current systems present, it is difficult to replicate the model environment where these can be carried out without noise and photon loss. This method incorporates all the widely used protocols, which come together in a way they fit to form the model way data is transmitted.

The viability of this doesn't seem applicable right now, but in the near future, when it is viable, it can be incorporated into every small thing, which can then enhance the security that we have today. When we start incorporating quantum computing to decrease error rates, quantum annealing to find the best path and also use the least energy while carrying out all the processes, we won't only have very less energy consumption but also have our sensitive information traveled in the most secure way.

References

[1] Nielsen MA, Chuang IL. *Quantum Computation and Quantum Information*. Cambridge University Press; 2000.

[2] Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. In: *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, India. New York, NY, USA: IEEE; 1984; p. 175–179.

[3] Shankar R. *Principles of Quantum Mechanics*. Springer Science & Business Media; 1994.

[4] Gisin N, Ribordy G, Tittel W, et al. Quantum cryptography. *Rev Modern Phys*. 2002;74(1):145. doi:10.1103/RevModPhys.74.145.

[5] Lo HK, Ma X, Chen K. Decoy state quantum key distribution. *Phys Rev Lett*. 2005;94(23):230504. doi:10.1103/PhysRevLett.94.230504.

[6] Albash T, Lidar DA. Adiabatic quantum computation and quantum annealing: theory and practice. *Rev Modern Phys*. 2018;90(1):015002. doi:10.1103/RevModPhys.90.015002.

[7] Das A, Chakrabarti BK. Colloquium: quantum annealing and analog quantum computation. *Rev Modern Phys*. American Physical Society, College Park, MD, USA; 2008;80(3):1061. doi:10.1103/RevModPhys.80.1061.
[8] Farhi E, Goldstone J, Gutmann S, et al. Quantum computation by adiabatic evolution. *arXiv preprint quant-ph/0001106*; 2000.
[9] Griffiths DJ. *Introduction to Quantum Mechanics*. Pearson Education; 2005.
[10] Lucas A. Ising formulations of many NP problems. *Front Phys*. Lausanne, Switzerland: Frontiers Media SA; 2014;2:5. doi:10.3389/fphy.2014.00005.
[11] Scarani V, Bechmann-Pasquinucci H, Cerf NJ, et al. The security of practical quantum key distribution. *Rev Modern Phys*. 2009;81(3):1301. doi:10.1103/RevModPhys.81.1301.
[12] Ekert AK. Quantum cryptography based on Bell's theorem. *Phys Rev Lett*. 1991;67(6):661–663. doi:10.1103/PhysRevLett.67.661.
[13] Johnson MW, Amin MHS, Gildert S, et al. Quantum annealing with manufactured spins. *Nature*. London, UK: Nature Publishing Group; 2011;473(7346):194–198. doi:10.1038/nature10012.
[14] Yamamoto N, et al. Evaluating quantum annealing for cryptographic applications. *Quantum Inf Process*. 2020;19(3):120.
[15] Rosenberg G, et al. Quantum annealing and its potential impact on cryptographic security. *J Quantum Inf Sci*. 2016;6(1):19–25.

About the Authors

Aadi Shah is a student in 11th grade at the Jayshree Periwal International School in Jaipur, India. Mr. Shah has a passion for Technological Innovation and Entrepreneurship. His particular interest is in Quantum Physics and Computer Science, where he seamlessly connects theoretical knowledge to practical applications. Developed in collaboration with over ten NGOs. Mr. Shah is a dedicated change-maker. Whether leading beach clean-ups or creating algorithms for rescuing animals, leadership inspires those around him. Aadi's keen interest in learning the World of Quantum Mechanics makes him passionate about diving into the world of quantum computing from various angles.