DTL REPORT

Topic: Quantum Computing

By:
Rahul Patnaik (1RV23CD041)
Noel Shaji Mathew (1RV23CD034)
Aditya Bhandari (1RV23CD003)

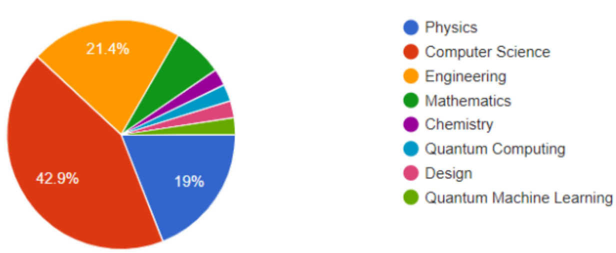
Table of Contents

Phase 1: Empathy

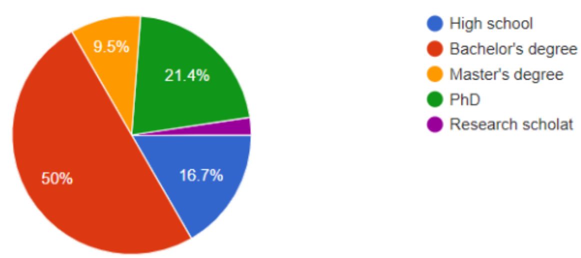
Stakeholders

Our stakeholders consisted of: **Students**, **Professors**, **Daily commuters**, **Researchers (From research based companies)**. Our largest stakeholders were students and daily commuters. We got details about them through our surveys.

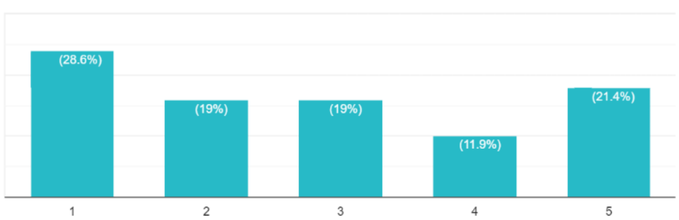
1) Fields they work in:



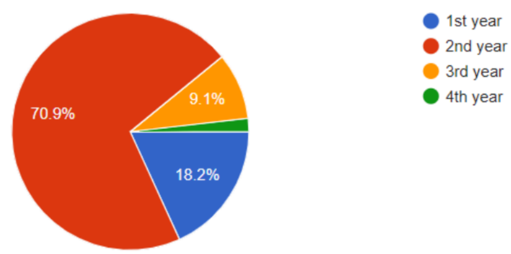
2) Educational background:



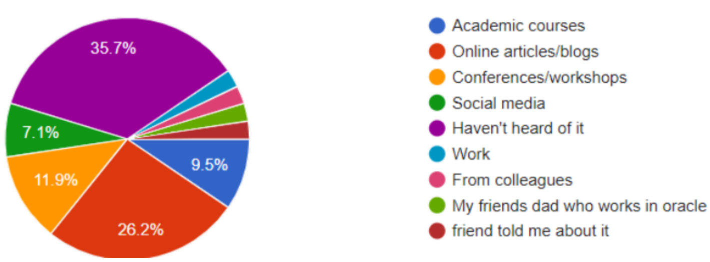
3) Familiarity with quantum annealing:



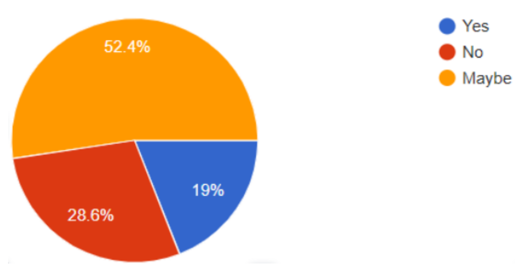
4) Year of study:



5) How they heard about quantum computing:



6) Belief in quantum computing:



Our target audience

We identified that our target audience would be:

- Large scale businesses
- Government agencies
- Researchers

Current optimization applications

- Used by Volkswagen for Logistics and traffic optimization.
- Monte Carlo Problem.
- Siemens and GE to optimize power grids
- Biogen and D-wave for drug discovery.

Questions asked in the survey

- Problems faced daily that could need automation?
- Knowledge about few solutions offered
- Bottlenecks in existing technology for these problems
- In your opinion, how significant is the potential impact of quantum annealing on industry and research?
- Do you think quantum annealing will become a mainstream technology and if so, where would its potential applications be?
- What do you see as some of the main challenges facing quantum computing

Questions asked in the interviews

- Problems faced daily that could need automation?
- Knowledge about few solutions offered
- In your opinion, how significant is the potential impact of quantum annealing on industry and research?
- Do you think quantum annealing will become a mainstream technology and if so, where would its potential applications be?
- What do you see as some of the main challenges facing quantum computing
- What are the best practices for integrating quantum annealing into hybrid classical-quantum algorithms, especially when using hybrid solvers? How should one handle cases where classical optimization algorithms dominate, and the quantum contribution appears minimal?

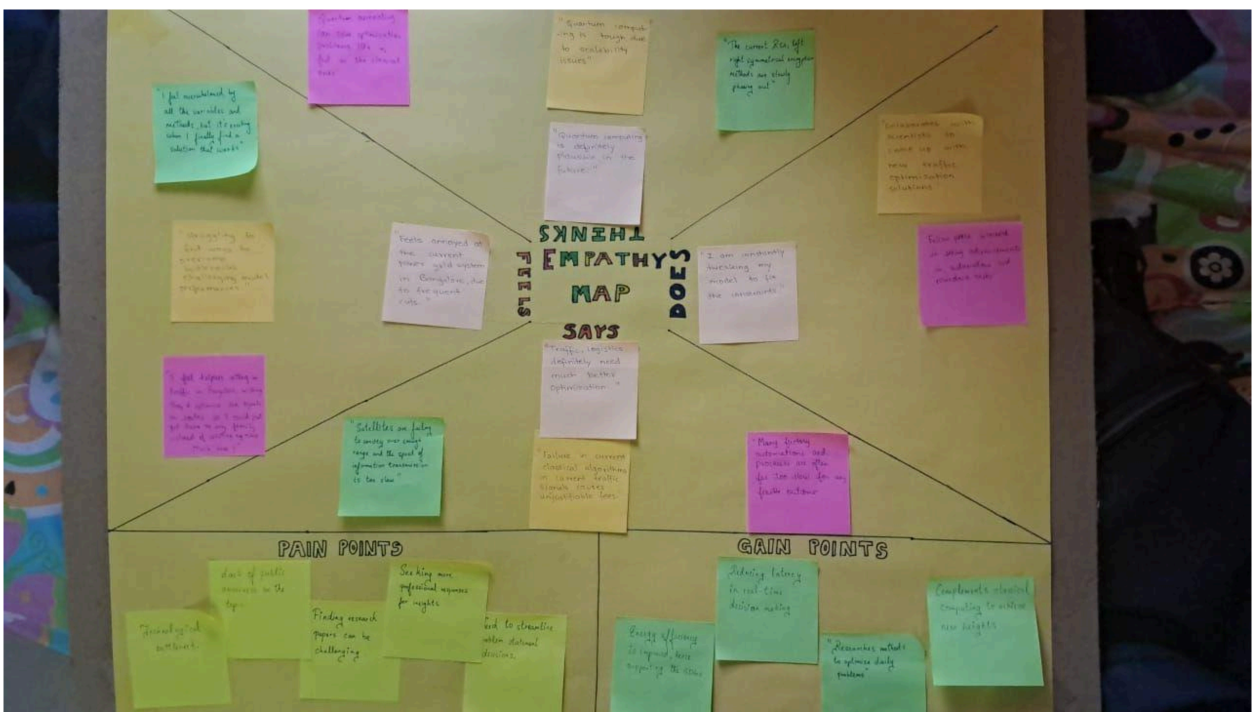
- How do we optimally map combinatorial optimization problems onto a quantum annealer for complex real-world applications? For instance, in cases where the problem graph topology doesn't match the hardware (Chimera or Pegasus graph)

Journey

This is how we went about to gain intuition:

- We developed the surveys to find out where optimization can be applied on real world problems (such as traffic, manufacturing)
- We emailed various Indian quantum computing start-ups to request interviews.
- Conducted interviews with students to gather insights.
- Reviewed a few research papers
- Analyzed survey responses to identify key themes.

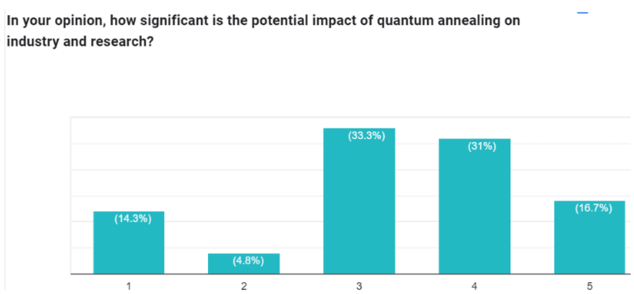
Empathy map

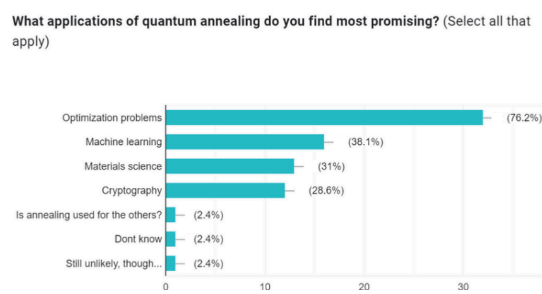


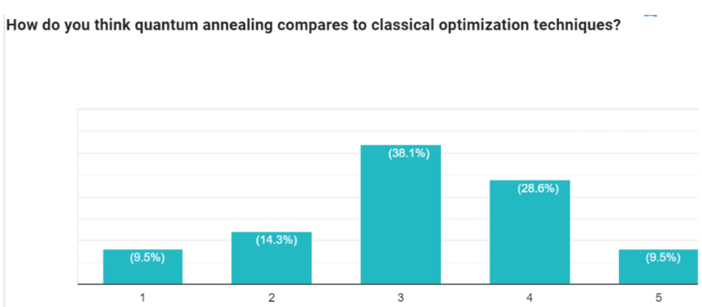
Phase 2: Define

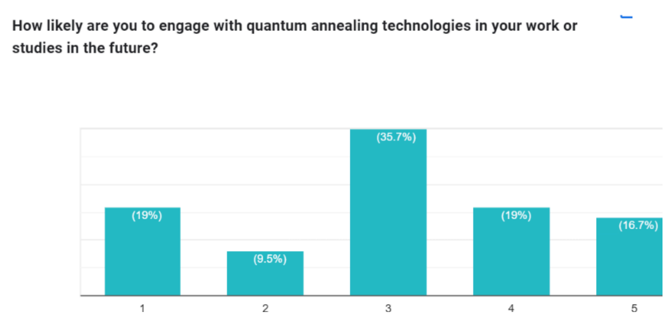
Insights gained from the survey

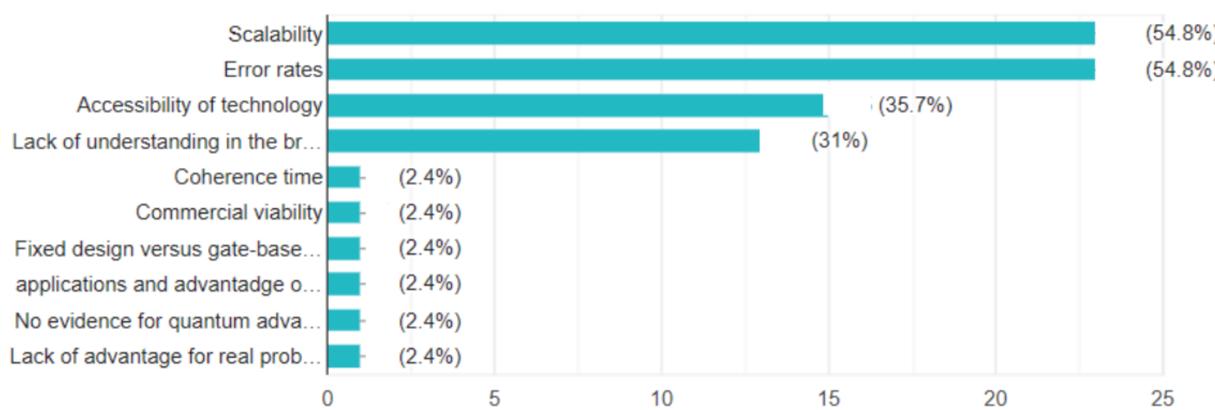
- Accessibility and understanding for a wider audience
- Use with other quantum computing techniques
- Large scale
- Use alongside AI and cryptography
- Specialized qubits
- Applications in drug discovery and logistics
- Determination of error rates
- Ability to represent larger problems
- Rigorous benchmarking
- Finding a class of problems suitable for applying quantum annealing
- We asked respondents about various daily issues, ranging from the traffic they face daily to the manufacturing industry in India and much more.
- Several interviews suggested many simple daily problems - delivery, traffic, mobile network, etc.. seemed to hamper their enjoyability in life.
- Upon asking about current areas where optimization could become a huge improvement or necessity we received these were the top 3 results :
    - Traffic jams
    - Drug discovery
    - Improving satellite placements to maximize coverage
- To tackle a few of these issues such as traffic, mobile networks, drug discovery - we suggested different methods of optimization which included:
    - Classical Machine Learning
    - Quantum Computing (Specifically quantum annealing)
    - A hybrid mix of both
- We received an overwhelming majority suggesting classical optimization methods for the given solutions, often stating that quantum-based solutions had scalability issues.
- But, we received many responses stating that the classical methods are often erroneous and do not work as intended accurately.











Insights gained from a company

- "Initially, we were uncertain about the best direction to take in quantum computing, especially when it came to choosing the right approach. However, insights gained from the company helped us clarify our path. They highlighted that quantum annealing hardware is not only more widespread but likely to be well-developed far sooner than quantum gate hardware. Their guidance also helped us identify key applications and areas for improvement, shaping our understanding and supporting us throughout this journey in quantum computing."

Insights gained from a professional

- Treat quantum annealing as an exploratory tool. While classical solvers might dominate now, quantum annealing can reveal insights into alternative solution pathways that classical algorithms might miss. These insights might not be substantial today but could become critical as quantum hardware improves.
- Hybrid solvers often switch between classical and quantum optimization cycles. You should iteratively refine your solution by leveraging quantum annealing for certain optimization steps, such as local search or heuristic improvement, while relying on classical solvers for larger, deterministic portions.

Insights gained from professionals through the survey

- Classical optimizers already do a fantastic job. if you look at the industry relevant problems in the field it's not worth it to "maybe" get a moderate improvement from an expensive quantum annealer using heuristics. Extremely skeptical of DWave's business and anyone else that claims they get advantage from their machine
- We use quantum annealing to sample large combinatorial optimization problems. It very effectively returns solutions that meet our constraints and maximize the objective. The ability to represent 10x larger problems would make it a solid alternative to classical sampling...
- Simulating QA on conventional hardware does yield better solutions than conventional SA in some cases but takes too much time to be practical. Need a working, scalable, accessible, affordable quantum computer for industrial applications.

Our conclusions

- Traffic, drug discovery and many more daily problems require automation and optimization.

- Classical optimization is good but needs practical rescaling.
- Annealing may not become a mainstream technology but is beneficial when used in combination with classic methods

Pain points

Here is where we lacked:

- Seeking more professional responses for insights.
- Need to streamline problem statement decisions.
- Finding research papers can be challenging.
- On a positive note, we received encouraging feedback from our professor

Our user persona

About:

Janet Snyder, 35, is a marketing manager in San Francisco who relies on messaging apps for work and personal use. After experiencing a privacy breach that leaked sensitive business information, Janet has become cautious about data security. While not tech-savvy, she values apps that provide strong privacy protections with easy-to-use interfaces.

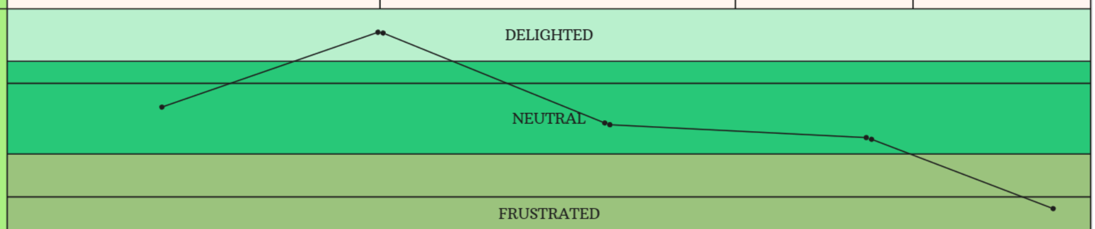
Motivation:

- Trust in apps with proven security (e.g., Quantum Key Distribution).
- Effortless communication without compromising privacy.
- Clear, accessible information about data protection.

End goals:

- Privacy breaches and vague security claims.
- Overcomplicated or poorly integrated security features.
- Use secure messaging apps to protect sensitive data.
- Balance privacy with efficiency in daily communication.

User journey map

	Morning	Journey Phase	Afternoon	Evening
User Actions (Activities)	Person wakes up and starts their day by checking work emails and notifications.	Person tries to send confidential work documents while commuting.	Person encounters delays in file transfers or receives notifications about potential data breaches.	Person uses a messaging app to send personal messages but remains worried about privacy risks.
Sentiments (Thought Bubbles)	"Today's the day to get things done securely!"	"Why is the file transfer taking so long? Is it even safe?"	"I hope my client's sensitive data doesn't get intercepted... but who knows?"	"Why can't messaging apps guarantee my data stays private?"
Emotions (Mood Meter)				
Possible Solutions (Opportunities to improve the experience)	Ensure seamless integration of QKD-enabled secure communication tools in messaging apps.	Develop real-time quantum-encrypted file-sharing systems with instant verification of data safety.	Use quantum gates for faster data processing, ensuring reliability even under weak signals or high traffic.	Introduce end-to-end encrypted messaging platforms powered by QKD, giving users peace of mind for both work and personal communication.

Phase 3: Ideation

Potential ideas

- Dynamic traffic signal control
- Optimal satellite positioning to maximize signal coverage
- Optimize traffic flow to ease congestion
- Predictive maintenance scheduling for traffic infrastructure
- Optimized city planning based on traffic and population data
- Optimizing investment portfolios
- Fraud detection
- Optimizing risk assessment models for better financial forecasting
- Accelerating the discovery of new materials with specific properties
- Supply chain optimization
- Optimizing treatment plans
- Speeding up drug discovery
- Optimizing the dosage distribution in cancer therapy
- Optimizing distribution of electricity in smart grids
- Optimizing extraction efficiency of oil to reduce environmental impact
- Optimizing battery charging and discharging cycles for efficient usage\
- Optimizing cargo loading and unloading
- Optimizing air traffic flow and schedules
- Optimizing placement of sensors to monitor endangered species
- Optimizing pollution control
- Dynamic Pricing for businesses
- Hyperparameter tuning in Machine Learning
- Optimization of Cryptographic algorithms
- Enhancing network intrusion detection systems
- Waste management cycle optimization
- Optimizing water distribution networks.

Best idea

We finally decided on the idea: “Data Compression and Transmission: Optimizing data compression algorithms and transmission schedules”. The advantages of implementing this are:

- Energy efficiency

- Handling larger data
- Reducing Costs
- Faster Data Relay

Worst idea

The worst idea we found was: “Wildlife Tracking: Optimizing the placement of tracking devices and sensors in conservation areas to monitor wildlife movements and protect endangered species”. This was not a good idea due to:

- Simplicity of the Problem
- Availability of Classical Solutions
- Cost and Infrastructure
- Unpredictable Variables

Potential prototypes

- Quantum annealer using D-wave API
- Quantum gate based compression and quantum key distribution (QKD)
- Quantum-Assisted Sorting Algorithm for Secure Packet Prioritization

Out of these 3, we finalized on “Quantum gate based compression and quantum key distribution”. Here is some justification to that:

Why we did not implement quantum annealer using D-wave API

- Quantum annealing, although supported by multiple libraries, is hard to implement due to API reliance constraints.
- Quantum annealing is often slower than Quantum gate based operations.
- Flexibility in Algorithm Design
- Security Applications

Why we did not implement Quantum-Assisted Sorting Algorithm for Secure Packet Prioritization

- No Compression
- It lacks a robust security mechanism like QKD or entanglement-based protection.

- Focused only on sorting and prioritization, with no broader implications for overall data transmission efficiency or cryptographic security.

Why we decided on Quantum gate based compression and QKD

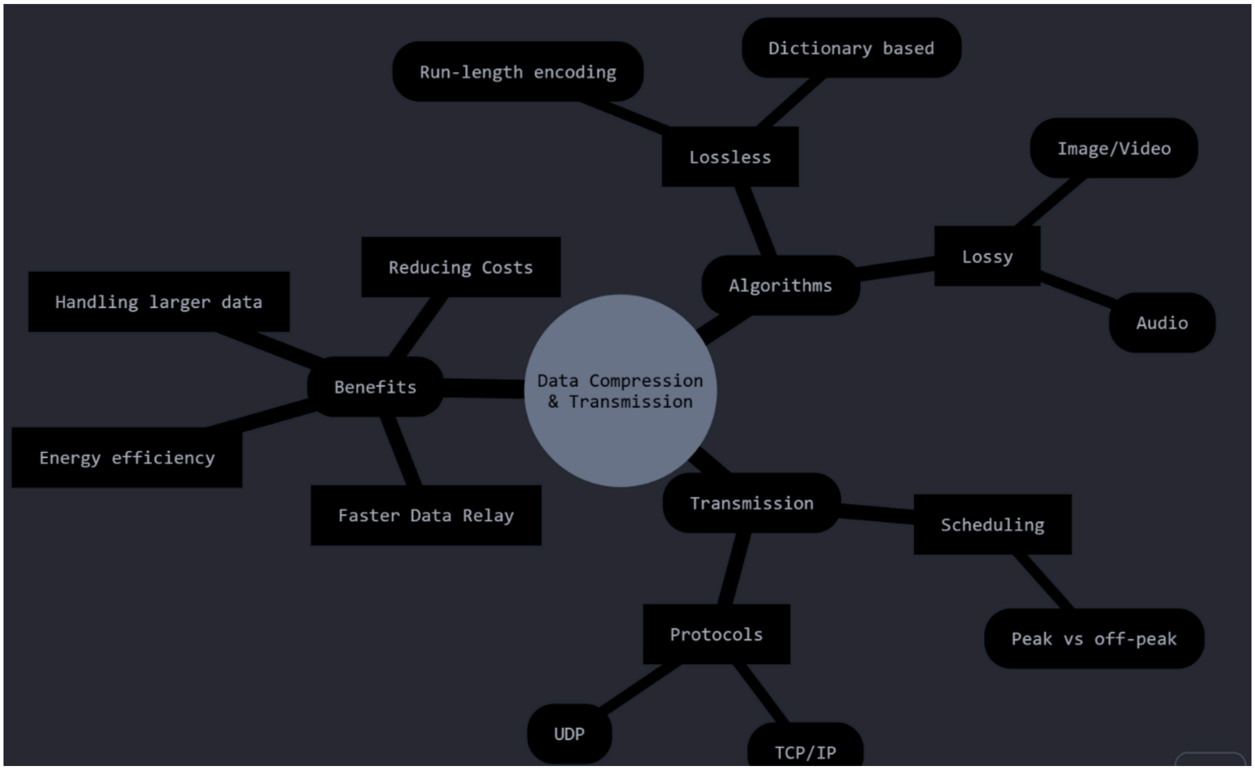
- Quantum gates are the basis of the new and upcoming quantum computers.
- Quantum Key Decryption allows us to ensure a strong encryption for the data, ensuring no-one may be able to snag the data from us.
- It is faster than quantum annealing where we must optimize the energy states by minimizing the energy at all levels.
- It is more easily compatible with binary numbers.

Important advantages

- Classical encryption cannot protect data from damage, as eventually a bigger number can be broken as always.
- Data transmission usually done in chunks can now be sent at multiple chunks at the same time in parallel.
- If the key is measured, it implies eavesdropping which means very strong security.

Brainstorming

Mind map



Data Compression & Transmission
Benefits
Handling larger data
Reducing Costs
Energy efficiency
Faster Data Relay
Algorithms
Lossless
Run-length encoding
Dictionary based
Lossy
Image/Video
Audio
Transmission
Scheduling
Peak vs off-peak
Protocols
UDP
TCP/IP

Phase 4: Prototyping

Libraries used

- json
- heapq
- defaultdict
- flask
- pennylane
- numpy

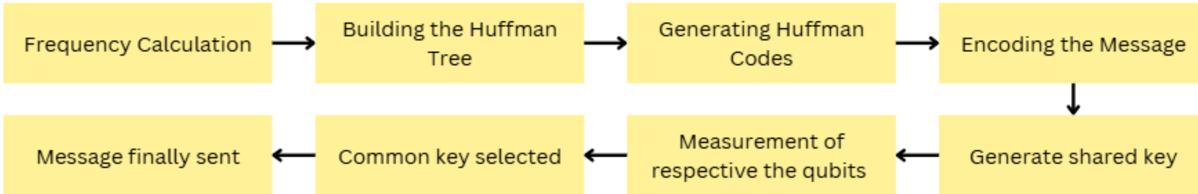
Huffman encoding

- Each bit of the Huffman-encoded stream is mapped to a quantum state: 0 → $|0\rangle$ and 1 → $|1\rangle$
- This stream of qubits is initialized in a quantum register.
- Pairs of qubits are entangled using the CNOT gate. This ensures that interception of qubits is detectable.
- The encoded qubits are passed through a Hadamard gate, creating superpositions $|0\rangle + |1\rangle$. This enhances the transmission by allowing multiple bits of information to be represented simultaneously.
- Quantum gates for error correction protect against noise during transmission.

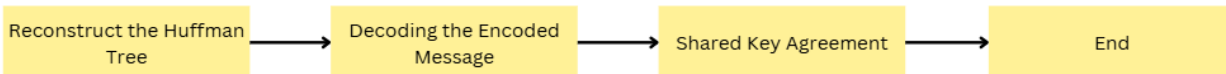
Quantum key distribution

- It uses the BB84 protocol to securely share a key. Qubits are encoded in random bases via Hadamard gates. The receiver measures qubits in random bases and publicly compares results to verify matching bases. A shared secret key is established without direct transmission.
- Huffman data and the QKD key are sent over a secure quantum channel. The receiver decodes the data using the reverse Huffman table. Any eavesdropping is detected by measuring fidelity with expected entangled states.

Flow of encryption:



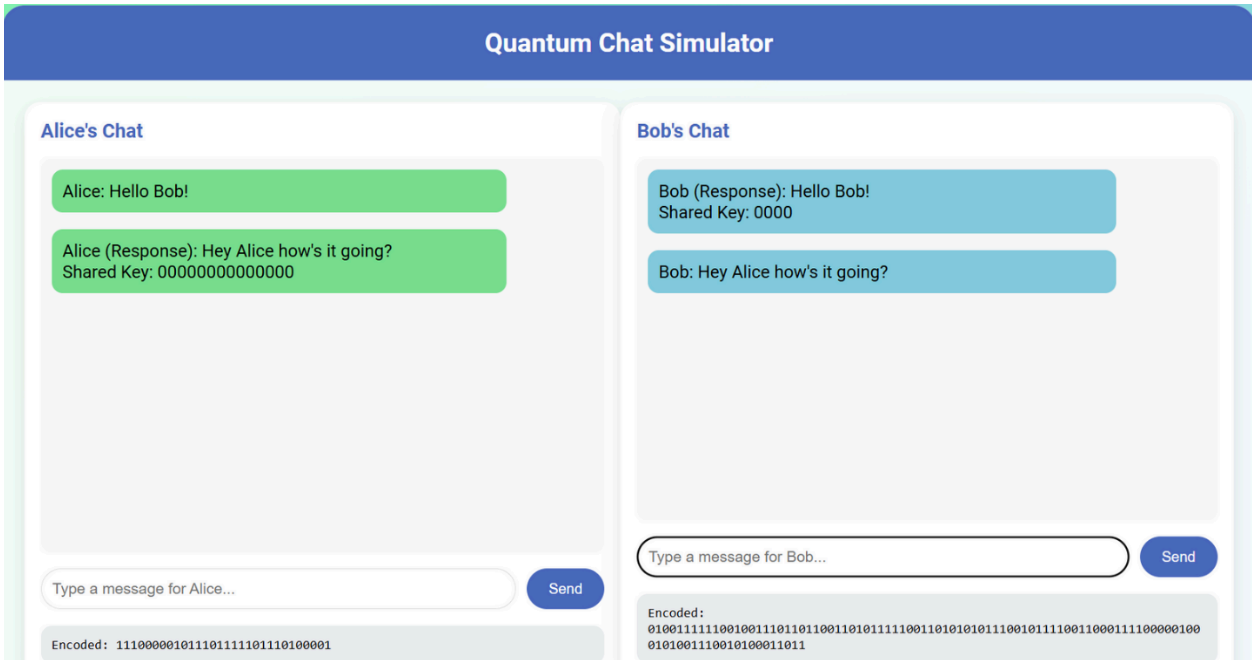
Flow of decryption:



Applications

- Secure Satellite Communication: Compressing and securely transmitting massive data streams between Earth stations and satellites.
- Quantum Internet: Building a scalable and efficient quantum communication framework for real-time data exchange.
- Healthcare Data Transmission: Securing sensitive medical data like DNA sequences or MRI images using quantum-enhanced Huffman encoding.

Working of the prototype



Google Colab Notebook representing the Data-transmission and security:

Link:
https://colab.research.google.com/drive/1xuQ4qxvZ340DtCWxx6gLBkn8tFvg_ebw?usp=sharing

Click the above link to access the concept we have utilized. The main code is available as a folder in the drive.

Phase 5: Testing

Validation and testing

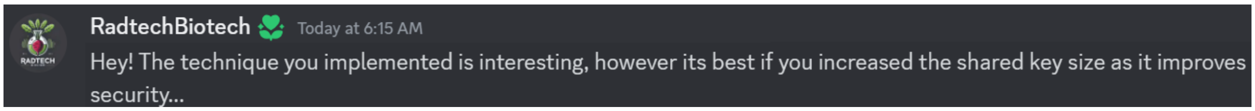
- **Friend Network Testing**
  Invited friends to interact with the system, providing feedback on message clarity, response accuracy, and functionality in various scenarios.
- **Community Platforms**
  Shared a test version on platforms like Discord and Reddit, collecting diverse user feedback and suggestions for improvement.

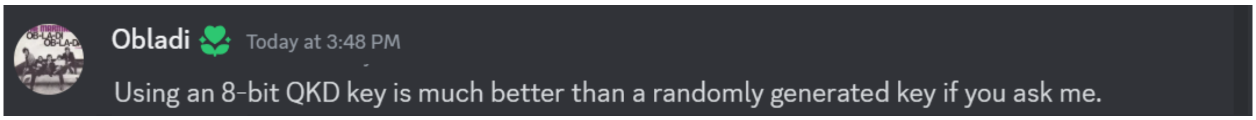
Teamwork and participation

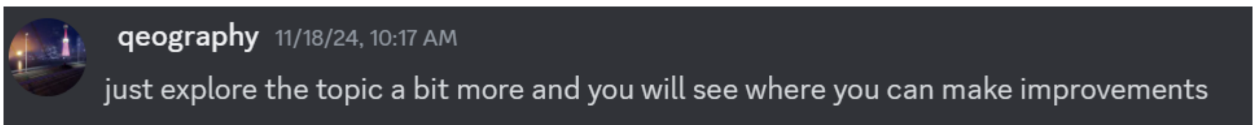
- **Quantum Annealing Research & Design**
  One team member spearheaded the research on quantum annealing techniques, focusing on optimizing message transmission for speed and security. Their work involved designing a theoretical framework that applied quantum principles to reduce transmission time and address security vulnerabilities, forming the core foundation of the project.
- **QKAD Development & Algorithm Optimization**
  Another team member took the theoretical research and translated it into a functional system. They implemented the QKAD algorithms, ensuring the message encoding and decoding processes were optimized for both efficiency and security. Additionally, they integrated quantum error correction techniques to enhance the system's reliability and robustness, ensuring that the system could withstand the inherent noise in quantum systems.
- **User Testing & Feedback Integration**
  One member led the testing phase, managing user interactions on platforms like Discord, Reddit, and through direct feedback channels. The testing assessed the system's performance in real-world scenarios, with users offering insights into the user interface, system responsiveness, and functionality. This phase was essential for identifying usability issues and technical flaws. He analysed the feedback to guide improvements, refine performance, and ensure QKAD was user-friendly and met practical needs. I also monitored performance metrics to ensure the system could handle

various use cases and network conditions, enhancing its versatility and reliability.

Some feedback we received from online forums







We understood that we would have to increase the key size to ensure safety of transmission. We also found that we could try out various other compression-decompression algorithms.

Impact Analysis

- **Enhanced Data Security**
  By integrating quantum key distribution with Huffman encoding, we ensure unprecedented levels of security. This approach is resilient against both classical and quantum attacks, safeguarding sensitive information in critical applications like healthcare, finance, and defense.
- **Energy Efficiency**
  Leveraging quantum superposition and entanglement enables efficient data compression and parallel transmission, reducing energy consumption compared to classical methods.
- **Scalability for Large Data Sets**
  Our system can handle increasingly larger volumes of data, making it suitable for industries such as satellite communication, where massive streams of information need to be transmitted securely and efficiently.
- **Quantum Technology Adoption**
  By demonstrating a practical use case, this project encourages broader adoption of quantum computing technologies, especially in hybrid systems combining classical and quantum methods.
- **Future-Proofing Against Emerging Threats**
  With advancements in quantum computing, classical encryption methods

may become obsolete. Our system anticipates and addresses this challenge by incorporating quantum-resilient encryption techniques.

How can we Upscale Our Project?

- **Collaboration with Industry Leaders**
  Partnering with quantum computing companies like IBM, D-Wave, or Rigetti could provide access to advanced quantum hardware and expertise, accelerating development and deployment.
- **Integration with AI for Intelligent Data Compression**
  Incorporating AI-driven algorithms could further optimize data compression by identifying patterns and redundancies, enhancing efficiency beyond traditional methods.
- **Developing Cross-Platform Compatibility**
  Ensuring that our solution works seamlessly across various quantum hardware platforms (e.g., superconducting qubits, photonic qubits) would expand its usability.
- **Expanding to New Use Cases**
  Exploring applications in smart cities (e.g., optimizing IoT data transmission), financial systems (e.g., secure transaction protocols), and global communication networks (e.g., quantum internet infrastructure).
- **Implementing Advanced Error Correction Techniques**
  Adding more robust quantum error correction mechanisms would improve reliability, especially in noisy quantum environments.
- **Public-Private Partnerships**
  Collaborating with government agencies and research institutions to implement pilot projects in critical areas like defense communication and healthcare.
- **Education and Training**
  Hosting workshops, hackathons, and training sessions could build a community of developers and researchers to contribute to and refine the system.
- **Open-Source Contribution**
  Making our libraries and prototypes open-source would encourage global collaboration and accelerate advancements in quantum-enhanced data transmission.

Conclusion

The implementation of Quantum Key Distribution (QKD) and Quantum Gate-based Data Transmission in secure communication systems marks a transformative leap toward robust data privacy and security. By leveraging quantum principles, this project successfully demonstrates a future-proof solution to vulnerabilities posed by traditional encryption methods.

Through the integration of QKD for unbreakable key exchanges and quantum gates for efficient data handling, the system ensures not only the confidentiality but also the integrity of transmitted information, even in dynamic or high-risk environments. This advancement addresses the growing concerns of users facing data breaches and privacy risks in daily communication, offering a practical, scalable approach to secure data transmission across industries.

In conclusion, this project showcases the immense potential of quantum technologies to redefine the standards of digital communication, paving the way for widespread adoption in sectors requiring uncompromising security, such as healthcare, finance, and government operations. With further refinement and collaboration, this innovation can become an essential pillar of secure communication in the quantum era.