Design Thinking Lab (CS237L) Report

Topic: Quantum Computing

Quantum-gate based compression & Quantum Key Distribution (QKD)

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

Faculty Mentors:
Dr. Shanta Rangaswamy
Dr.Soumya. A

RV COLLEGE OF ENGINEERING® BENGALURU-59

(Autonomous Institution Affiliated to VTU, Belagavi)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Certificate

Certified that the Design thinking Laboratory work titled ***"Quantum-gate based compression & Quantum Key Distribution (QKD)"*** is carried out by in partial fulfilment for the requirement of degree of **Bachelor of Engineering in Computer Science and Engineering** of the Visvesvaraya Technological University, Belagavi during the year 2024-2025. It is certified that all corrections/suggestions indicated for the Internal Assessment have been incorporated in the report.

Dr. Shanta Rangaswamy,	**Dr. Soumya,**	**Dr. Ramakanth Kumar P**
Professor, **Department of CSE**	**Associate Professor,** **Department of CSE**	**Professor and HoD,** **Department of CSE**

External Viva

Name of Examiners	Signature with Date
1.	
2.	

Declaration

This report has been prepared on the basis of our own work. Where other published and unpublished source materials have been used, those have been acknowledged.

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

Date of Submission:
Jan 6, 2025

Signature/s:

Abstract

Quantum computing is revolutionizing the landscape of secure communication and optimization applications, addressing critical challenges in data privacy, energy efficiency, and scalability. The integration of quantum key distribution (QKD) and quantum gate-based data transmission offers a transformative leap in securing sensitive information, particularly as traditional encryption methods face obsolescence in the quantum era. This project emphasizes the potential of quantum technologies to redefine data security standards, enabling robust communication frameworks for high-stakes sectors like healthcare, finance, and defense. With advancements in quantum hardware and hybrid methodologies, the project aligns itself with the evolving demands of an increasingly interconnected and data-driven world.

Focusing on real-world applications, this study combines theoretical exploration with practical implementation to demonstrate the viability of quantum computing in diverse domains. By leveraging quantum annealing for optimization problems and gate-based approaches for secure data transmission, the project showcases the breadth of quantum technologies in addressing challenges such as traffic flow management, drug discovery, and communication security. Prototypes developed with libraries like Pennylane and Flask highlight the practical feasibility of hybrid quantum-classical systems, bridging the gap between abstract research and tangible solutions. Insights gathered from extensive stakeholder engagement, including surveys and interviews with academia, industry leaders, and policymakers, revealed the pressing limitations of classical approaches and underscored the nascent promise of quantum computing. The iterative development process incorporated feedback from user testing and expert consultations, refining the prototypes to align with real-world demands. Quantum gate-based data compression emerged as a standout feature, offering unparalleled scalability and energy efficiency, while QKD was recognized as a cornerstone for next-generation cybersecurity protocols, ensuring resilience against future quantum threats.

The project addresses pressing issues such as privacy breaches, energy consumption, and scalability, showcasing quantum technologies' capability to overcome these challenges. The adoption of QKD ensures unbreakable key exchanges, while quantum gates optimize data handling for faster and more secure transmission. Feedback from user testing and expert consultations has refined the system, making it a viable solution for industries requiring uncompromising security and efficiency. This initiative underscores the transformative role of quantum computing in addressing global communication challenges, setting the stage for widespread adoption and innovation in the quantum era.

Acknowledgement

Any achievement, be it scholastic or otherwise, does not depend solely on the individual efforts but on the guidance, encouragement and cooperation of intellectuals, elders and friends. A number of personalities, in their own capacities have helped us in carrying out this Design Thinking Laboratory work. We would like to take this opportunity to thank them all.

We are also thankful to our mentors, Dr .Prafulla S B, Assistant Professor and Dr. Soumya A, Associate Professor, Dept. of CSE for their wholehearted support, suggestions and advice during this work.

Our sincere thanks to Dr. Ramakanth Kumar P., Professor and Head, Department of Computer Science and Engineering, RVCE for his support and encouragement.

We express sincere gratitude to our beloved Principal, Dr. K. N. Subramanya for his appreciation towards this work.

We thank all the teaching staff and technical staff of the Computer Science and Engineering department, RVCE for their help.

Table of Contents

Chapter 1: Empathy

1.1 Preamble: Introduction to Empathy

The first stage of the Design Thinking process begins with the Empathy Phase. In essence, empathy is our ability to perceive the world through other people's eyes, to observe what they see, to feel what they feel and to experience what they undergo. Now that we understand the definition and need for empathy, our immediate reaction must be to decide on what topic to address. Although it's easy to point out flaws in multiple systems, it's difficult to narrow down our focus onto one primary goal. Given that the world is our oyster, it might be easy to get swayed in multiple directions while looking for the right goal to focus on. Luckily for us, one voice of reason is that we wanted to empathize with something that resonated with us too. Something we have lived through and would like to see a difference in. So we decided to target the field of education.

Currently education plays a huge role in our daily lives as students. Our world revolves around tests, labs, submissions, quizzes and our teaching faculty. This applies to our teaching faculty too, who have dedicated their lives to bettering the students' knowledge. For years we have been following the same curriculum with minor changes here and there but this is not the case in the last year. Education as we know it has taken a 180 degree turn and paradigm shifted into an online world. The once corridors that were brimming with the chatter of students are now quiet and empty. We have all been transported into the digital world where our life revolves around a desk and a laptop. With the new rapid advancement in technology because of the required new tools, it has forgotten the pressing concerns of its consumers.

In order to attain our goal, which is to solve a pertaining problem in society, it is necessary to understand the emotions of our stakeholders. Stakeholders are the target audience for our novel idea and in our case they are Students and Teachers. Although this seems like a small group of people, in reality they are a large group with varied interests and opinions. So our first task was to narrow down our audience for the purpose of this project.

We have decided to empathize with Engineering students, faculty members and researchers. This helped us understand their problems even better as students of an engineering college ourselves. The next step is to identify the grievances phased by our Stakeholders. It is vital to streamline the questions we would ask them to ensure we get the right information we require from them. It was very clear to us that this presing topic requires addressal, as students we can clearly identify the shortcomings of this new method of learning.

The vital learning from this phase is that sometimes we believe there is an issue and before asking those involved about their opinions, we jump to find a problem. But through the help of this design thinking process, we understood that the main issue we thought of tackling wasn't the real concern of our part-takers. This causes a change in plan and direction which was the aim of this process. After gathering the information from them, it is vital to group opinions to unanimously have one voice for each of the parties involved. This can be done using the empathy maps that we created. After understanding the problem, it is imperative that we find possible problem statements to work on and propose the same to them. A constant dialog with the stakeholders is key to a successful empathizing journey.

1.2 Customer Persona and Environment

Customer Persona represents the essential characteristics of the people we aim to support through our design thinking journey. It involves understanding the stakeholders who will ultimately benefit from the solution, ensuring their challenges, motivations, and frustrations are addressed effectively. This foundational step helps build a robust design thinking model by aligning with the real needs of stakeholders and incorporating their feedback throughout the process.

In our project, we defined our Customer Persona as researchers, businesses, and government agencies—stakeholders deeply involved in solving optimization problems using classical and quantum techniques. The insights gained from empathy activities helped us identify the critical pain points and aspirations of these groups. These personas are pivotal in addressing pressing optimization challenges like scalability, efficiency, and security.

The personas highlighted a significant gap in the usability of quantum computing technologies. Researchers struggle with the scalability of classical methods and accessibility to advanced quantum systems, while businesses face challenges in integrating quantum solutions into existing workflows. Additionally, issues such as the complexity of quantum implementations, limited practical applications, and concerns over cost were frequently expressed.

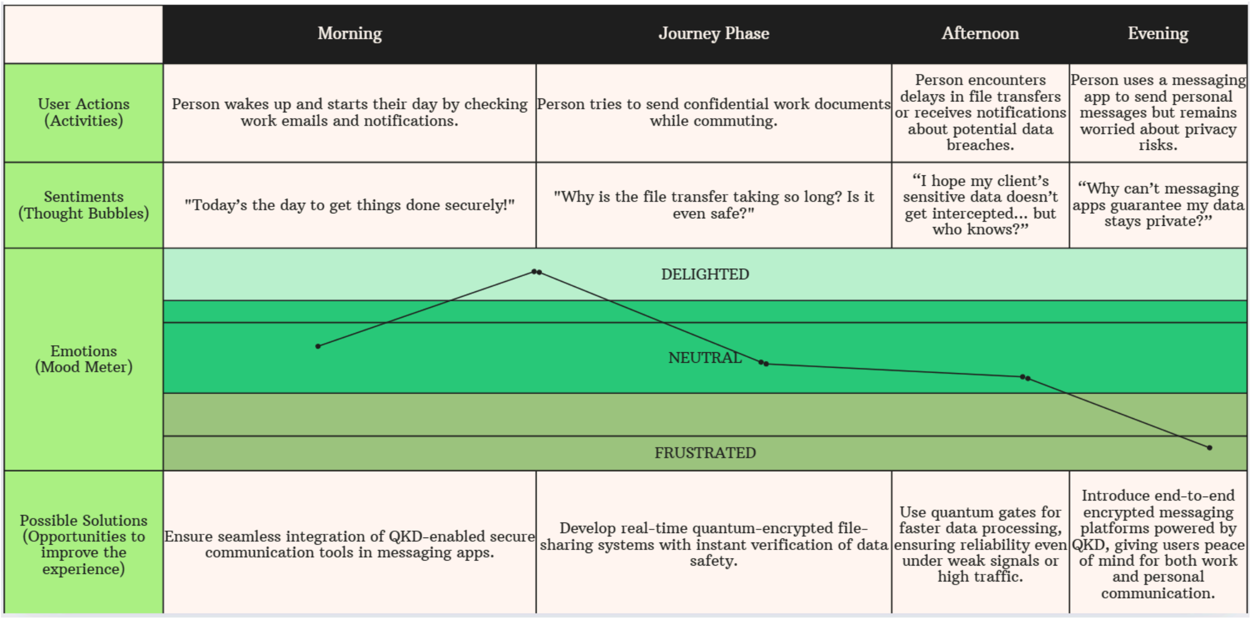
To address these challenges, our solution focuses on using Quantum Gate-Based Compression and Quantum Key Distribution (QKD) to provide secure and scalable data optimization systems. This approach tackles both the technical and practical limitations faced by our personas, such as enhancing real-time feedback mechanisms and reducing vulnerabilities in data transmission.

By focusing on these stakeholders and their specific needs, we aim to provide a solution that not only bridges the gap between classical and quantum systems but also ensures practical benefits for industries requiring robust optimization solutions. Our ultimate goal is to enable researchers and businesses to address real-world problems with a more accessible and impactful quantum approach.

This structured understanding of Customer Personas will help us stay aligned with the requirements of all our stakeholders, fostering a more comprehensive and beneficial design process.

1.3 User Journey Map

User Journey Map is a visualization depicting the various stages that the customers go through while interacting with an application developed.



	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)	DELIGHTED NEUTRAL FRUSTRATED			
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.

Figure 1. Customer Journey Map

1.3.1 Morning Phase:

- **User Actions**
  Person wakes up and starts their day by checking work emails and notifications.
- **Sentiments**
  "Today's the day to get things done securely!"
- **Emotions**
  Neutral, slightly positive as the day begins with plans for productivity.
- **Possible Solutions**
  Ensure seamless integration of QKD-enabled secure communication tools in messaging apps.

1.3.2 Journey Phase:

- **User Actions**
  Person tries to send confidential work documents while commuting.
- **Sentiments**
  "Why is the file transfer taking so long? Is it even safe?"
- **Emotions**
  Neutral, transitioning to frustration due to delays and concerns about security.
- **Possible Solutions**
  Develop real-time quantum-encrypted file-sharing systems with instant verification of data transfer safety.

1.3.3 Afternoon Phase:

- **User Actions**
  Person encounters delays in file transfers or receives notifications about potential data breaches.
- **Sentiments**
  "I hope my client's sensitive data doesn't get intercepted… but who knows?"
- **Emotions**
  Frustration as concerns about data safety intensify.
- **Possible Solutions**
  Use quantum gates for faster data processing, ensuring reliability even under weak signals or high traffic.

1.3.4 Evening Phase:

- **User Actions**
  Person uses a messaging app to send personal messages but remains worried about privacy risks.
- **Sentiments**
  "Why can't messaging apps guarantee my data stays private?"
- **Emotions**
  Frustration, with a desire for peace of mind regarding communication privacy.
- **Possible Solutions**
  Introduce end-to-end encrypted messaging platforms powered by QKD, giving users peace of mind for both work and personal communication.

1.4 User Empathy Maps

User Empathy Maps are used to gain perspective on the problem at hand, via the eyes of our user personas. It captures what the customer says, does, feels, and thinks, about the situation they've been presented with. User Journey Maps are especially important for understanding what are the most common problems faced by customers, and what they think could be a solution to said problem. Although it isn't feasible to inculcate every solution suggested by every customer, it does provide an insight into what could be worked on, to ensure that the maximum possible ideas are acquired, for a deeper understanding of the problem.

To make the empathy maps, we resorted to conducting interviews with students, professors as well as researchers to ensure that we could gather as much information as possible. By gauging out their views or perspective on these certain problems as well as get their feelings on the matter at hand.

To proceed with the empathy phase we curated google forms and in-person interviews with all the stakeholders at hand. The stakeholders were divided into three main categories:

- Students from within RV College of Engineering as well as outside.
- Researchers from universities in different colleges as well as companies.
- Professors within RV College of Engineering as well as other colleges.

Based on the feedback we received from them, we made our empathy maps, and also made a general empathy map for each category. From the empathy maps we were able to get a clear picture of what troubles students and teachers when it comes to sharing data between various people via any online platform.

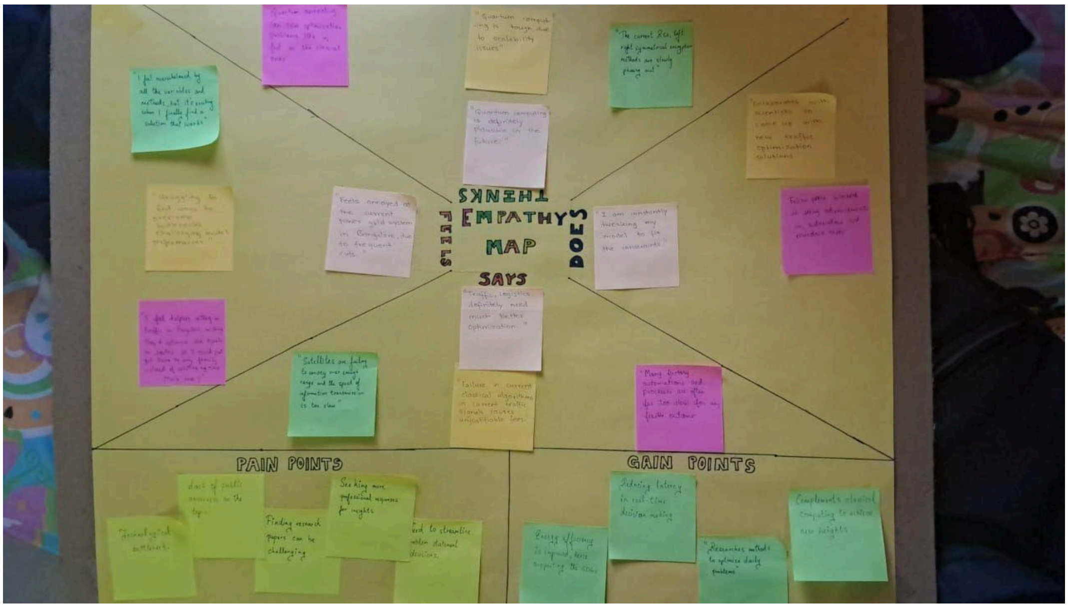


Figure 3. Empathy map

Conducting these interviews helped us see problems, which we might've never known, had we only worked from our perspective. It shed light on many matters, which may seem trivial on the surface, but by talking to teachers and students, we understood the gravity of the problems. It helped us identify the issues that are prevailing.

From our empathy maps, we took the most commonly suggested solutions by both teachers and students alike, filtered out the feasible and viable solutions and from there went on to generate ideas for the same.

1.5 Tools used for Empathy

1.5.1 Customer Survey and Analysis

We conducted a survey on google forms for this phase. 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.

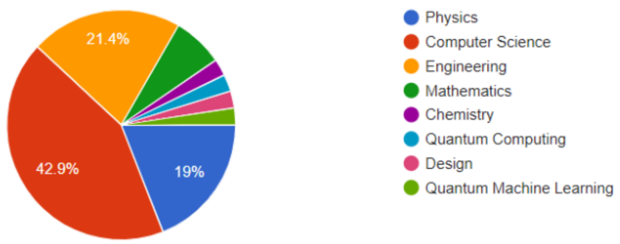


Figure 5. Survey Pie chart showing the educational fields

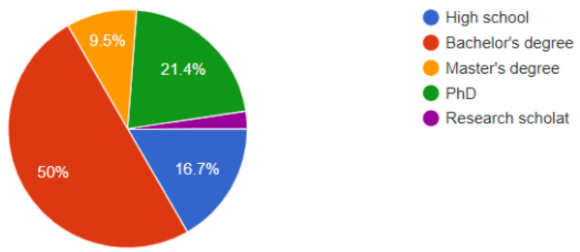


Figure 6. Survey Pie charts showing educational background

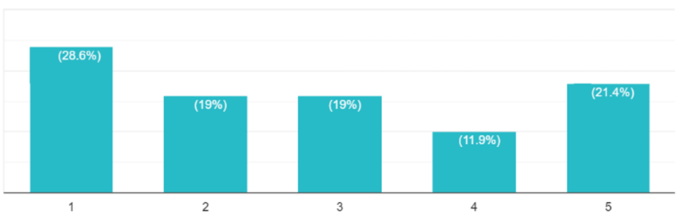


Figure 7. Bar graph showing familiarity with quantum annealing

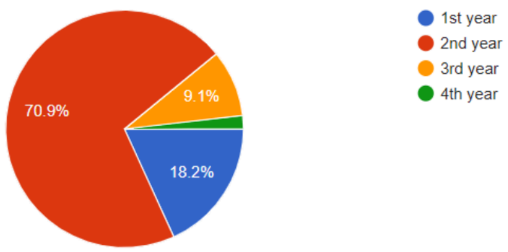


Figure 8. Survey Pie charts showing the year of study

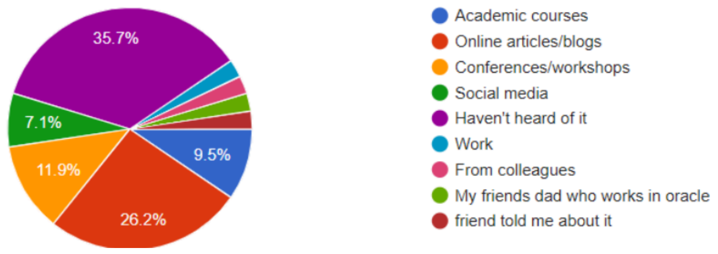


Figure 9. Survey Pie charts showing how they heard about quantum computing

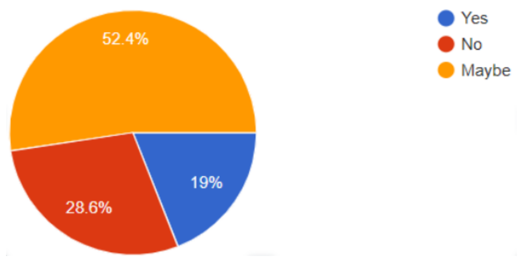


Figure 10. Survey Pie chart showing the belief in quantum computing

1.5.2 User Interaction Photos with descriptions

These are some of the pictures of our team interacting with a few students in interviews.

Figure 11. User Interaction during Interview

These images from Figure 11., depict our interactions with fellow students during our interview with them as part of our Empathy phase. We received a plethora of responses from the interviewees which has helped us in growing our problem statement and figuring our edge cases.

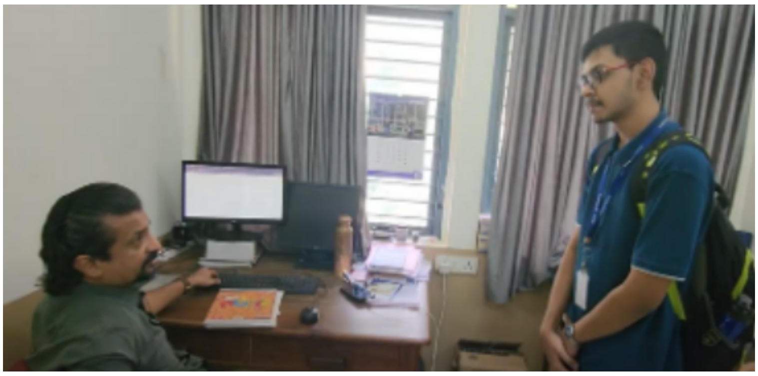


Figure 12. Interview with professor

Figure 12 depicts the image of our interview with professor, Karthik Shastry from the Department of Physics RVCE. Under his guidance, we were able to get a clear picture of our problems and find correlations between the problems and a few existing as well as potential solutions.

1.5.3 Customer Interview's details

Target audience

- 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.

Questionnaire for 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

Questionnaire for the Interview

- 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)

Methodology to gain insights regarding the potential problem statement

- Developed the surveys to find out where optimization can be applied on real world problems (such as traffic, manufacturing)
- 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.

Chapter 2: Define

2.1 Preamble: Introduction to problem definition

It is during the problem definition phase that the project is being fleshed out by the team. As a group we will be in conjunction with our clients and decide upon the main aim of the project. This aids in a better understanding of the requirements, goals, expectations and current progress in the field for us to be able to better the vision of the end result of our work. Although it's easy to define the process of this phase and what it contains, in reality it can be a very daunting task. To begin with, we realize the requirements of our stakeholders cannot be implementable concepts. They might expect a utopian solution to their grievances, but this is far from the realm of possibilities. This sparks the need for open communication with them to help them realize our limitations and the reach we have.

Sometimes we get carried away too by trying to find immediate solutions without properly defining in one-to two sentences about the real issue at hand. Without the glamorous words around the problem, it is vital to give everyone a glimpse of the main subject at hand. But what exactly would be a good problem definition? From our findings, it is a sentence that perfectly describes the need for the project and the issue it solves. From the problem statement we will then be able to find the possible solutions and then work on the implementation.

In our case, our problem statement needed to tackle the challenges of optimization in real-world applications, which often face bottlenecks due to the limitations of classical methods and the complexity of quantum solutions. To draft a statement, we looked into user requirements and had to eliminate suggestions such as quantum annealing hardware implementation using D-Wave API due to its scalability issues and API reliance constraints. Instead, we focused on areas where our group of three could make meaningful contributions with limited resources and restricted reach. This narrowed our focus to areas such as data compression and secure transmission, specifically leveraging quantum gates for compression and quantum key distribution (QKD) for enhanced security.

We began by investigating how current industries manage optimization challenges and the shortcomings they face. Questions such as how researchers approach the scalability of classical methods, how hybrid solvers integrate quantum components effectively, and what constraints limit the applicability of quantum solutions shaped our problem statement.

2.2 "How might we" questions

"How might we" questions are concise prompts designed to initiate brainstorming. These questions stem from our insights and design principles, acting as seeds for ideation. To be effective, a "How Might We" (HMW) question must strike a balance—broad enough to allow diverse solutions but narrow enough to provide useful boundaries for exploration. Based on our findings, we produced six key questions that encapsulate the scope of our project:

1. **How might we address scalability issues in classical optimization methods?**
   Classical methods are often limited in handling large-scale problems. This question explores the development of hybrid solutions that integrate quantum and classical optimization techniques to overcome scalability constraints.

2. **How might we leverage quantum principles to enhance data security?**
   Given the vulnerabilities of traditional encryption methods, this question focuses on utilizing quantum key distribution (QKD) to provide unbreakable security for sensitive data transmissions, addressing concerns from various stakeholders.

3. **How might we identify and tackle bottlenecks in optimization for real-world applications?**
   From traffic management to drug discovery, optimization challenges exist across industries. This question seeks innovative methods to pinpoint and resolve these bottlenecks, ensuring improved efficiency and reliability.

4. **How might we ensure compatibility between quantum and classical methods in hybrid systems?**
   The coexistence of classical and quantum techniques requires seamless integration. This question addresses the challenge of optimizing resource utilization while maintaining functionality and efficiency in hybrid solvers.

5. **How might we simplify the adoption of quantum solutions for non-experts?**
   Many professionals highlighted the complexity of quantum solutions. This question seeks ways to make quantum technologies, like quantum gate-based operations, more accessible and user-friendly for widespread adoption.

6. **How might we enhance real-time feedback mechanisms in quantum-assisted systems?**
   Drawing parallels to feedback systems in education, this question aims to improve quantum systems by incorporating real-time validation and error correction to address issues promptly and enhance user confidence.

2.3 Design thinking challenges identified

The final problem statement Point of View is: Stakeholders in optimization-based applications, such as researchers and businesses, need scalable, secure, and efficient methods because existing classical solutions often lack the robustness to handle modern challenges. Some of the problems identified by our stakeholders include:

2.3.1 Challenges Identified for Researchers and Companies

1. **Scalability Issues in Classical Optimization**
   Researchers and companies noted that classical methods, while effective for small-scale problems, fail to scale efficiently for complex real-world scenarios. Examples include traffic management and drug discovery, where classical approaches encounter significant bottlenecks.

2. **Insight**
   Survey responses revealed that large-scale applications require a combination of quantum and classical methods to ensure scalability.

3. **Security Concerns**
   Classical encryption methods are increasingly vulnerable to both classical and quantum attacks. Stakeholders expressed the need for robust security mechanisms like Quantum Key Distribution (QKD) to address these vulnerabilities.

4. **Insight**
   QKD offers unparalleled security by detecting eavesdropping attempts, ensuring data confidentiality.

5. **Limited Accessibility to Quantum Resources**
   Implementing quantum solutions, such as quantum annealing, remains challenging due to API constraints, hardware costs, and a lack of industry-standard tools.

6. **Insight**
   Developing hybrid solvers and accessible quantum systems can bridge the gap.

7. **Difficulty in Understanding Optimization Metrics**
   Without proper benchmarking and error rate determination, stakeholders struggle to identify areas where quantum solutions can outperform classical ones.

8. **Insight**
   Rigorous benchmarking and tailored use cases for quantum annealing can enhance understanding.

9. **Lack of Practical Examples**
   Several participants highlighted the need for tangible use cases and practical demonstrations of quantum technologies to understand their real-world applicability.

10. **Insight**
    Applications like optimizing satellite placements and drug discovery can demonstrate the potential of quantum technologies.

2.3.2 Challenges Identified for Students and Educators in Quantum Computing

1. **Complex Learning Curve**
   Quantum computing concepts are difficult to grasp for students without strong foundational knowledge. Educators also face challenges in effectively teaching these concepts due to a lack of intuitive teaching tools.

2. **Insight**
   Tools like simulations and simplified visualization can improve comprehension.

3. **Resource Constraints**
   Both students and teachers face issues accessing quantum hardware and software due to high costs and limited availability.

4. **Insight**
   Open-source frameworks and partnerships with quantum computing companies can address these constraints.

5. **Low Engagement Levels**
   Similar to the online education challenges, stakeholders expressed a need for interactive teaching methods to maintain interest and motivation.

6. **Insight**
   Gamification and project-based learning in quantum computing education can boost engagement.

7. **Absence of Hands-On Applications**
   Students felt unequipped to solve real-world problems due to a lack of practical exposure. Teachers noted the absence of tools to bridge the gap between theoretical learning and practical applications.

8. **Insight**
   Prototyping exercises like Huffman encoding and QKD implementations can offer hands-on learning opportunities.

By addressing these challenges, our project aims to demonstrate how quantum gate-based compression and QKD can provide scalable, efficient, and secure solutions, paving the way for broader adoption of quantum technologies.

Chapter 3: Ideate

3.1 Preamble: Introduction to Ideation

Ideation is an extremely creative process where designers generate ideas in sessions. It accounts as the third stage in the Design Thinking Process. We are expected to gather with open minds to produce as many ideas as possible to address the problem statement. The key to this phase is a judge-free, positive and supportive environment. This would definitely be one of the most exciting stages in the process, because the aim is to generate a large quantity of ideas that the team can then filter and cut down to finalize the final project.

It is very difficult to simulate a prejudice free environment when we ourselves have preconceived notions in our minds. First we need to unlearn the process of immediate opinion formation and have a third person perspective that is completely free of judgements. This concept gives rise to humorous and innovative ideas for brainstorming such as the worst possible ideas, SCAMPER and Braindump. Sometimes it's important to do many or all of the ideation processes before arriving at an exhaustive list of ideas. Sometimes even when the best minds merge, there may be ideas that are audience favourites and some only humour the one who owns it. Either way, emotions must be kept aside in terms of whose contribution is being recognized.Ultimately in the grand scheme of things, it doesn't matter who’s idea it is, but which idea is better.

These were some learnings we found while working on this phase. For our case, coming up with an exhaustive list of ideas seemed nearly impossible at first. But now reflecting, it was truly simple. We were able to make use of multiple ideation methodologies that expanded our mindset and gave us a new perspective. But another aspect of ideation is assimilating main ideas. After the creation of a list, proper tools must be employed to group these ideas into larger topics thereby streamlining our ideas. Ideation can be thought of as a branch and un-branch problem.

3.2 Ideation techniques used and description

There are a variety of ideation techniques that can be used for generation of ideas. Ideation techniques help in creative flow, and help in generation of a variety of ideas. Not all of these ideas may be good, but every idea in turn could lead to a better idea, and hence none of them can be neglected.

To generate ideas, we employed some well known ideation techniques that have been listed below. By employing these techniques, by the end of our ideation process, we were able to come up with over XX ideas! The techniques used by us for generation of ideas include:

- **Brainstorming Cloud**
  Brainstorming refers to a group of people just coming up with ideas and writing them down. It serves as a brain dump.
- **Worst Possible Ideas**
  These refer to ideas that, while not immediately practical or feasible, serve as catalysts for creativity and innovation. Such ideas push boundaries, challenging conventional thinking and inspiring new perspectives. By exploring these "impossible" concepts, teams can often uncover unique elements or approaches that can be adapted into actionable solutions, fueling the design process with fresh and unconventional insights.
- **Mind Map**
  A webbed map of all the problems and their possible solutions, for easy understanding. Figure 13, depicts our mind map for our ideation phase, assisting us with how we approach the ideas for our project

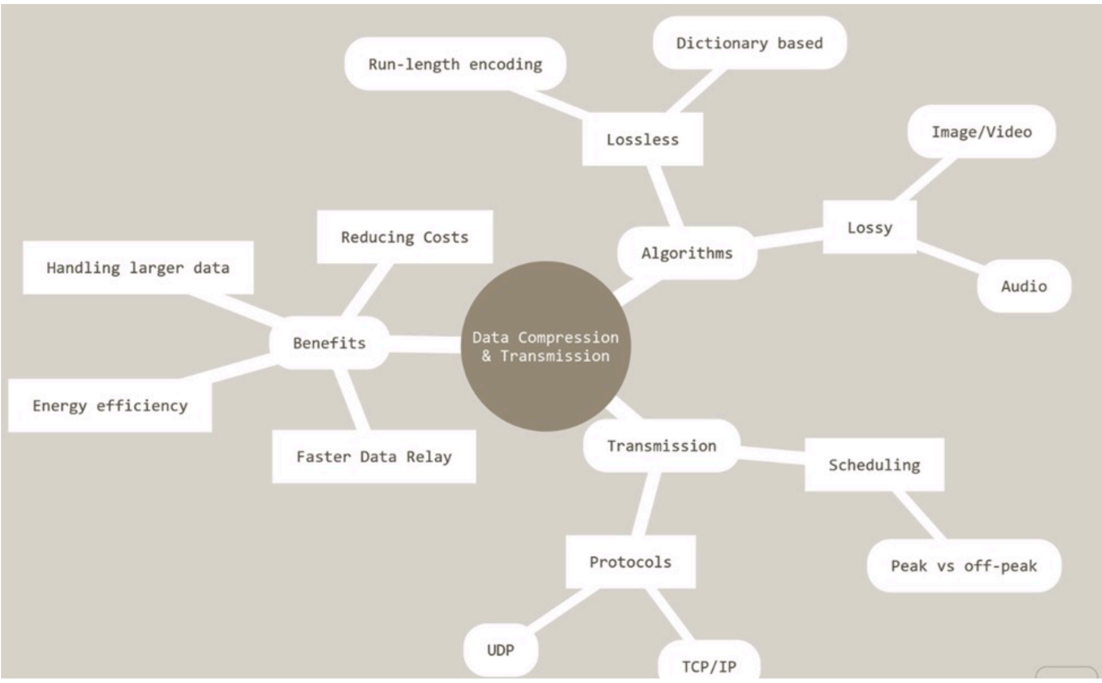


Figure 13. Mind Map for ideation

These techniques were very helpful, and allowed us to think differently and creatively. By employing the above ideation techniques, we were able to generate a plethora of ideas, which we've listed below.

3.3 Brainstorming potential ideas

1. Dynamic traffic signal control
2. Optimal satellite positioning to maximize signal coverage
3. Optimize traffic flow to ease congestion
4. Predictive maintenance scheduling for traffic infrastructure
5. Optimized city planning based on traffic and population data
6. Optimizing investment portfolios
7. Fraud detection
8. Optimizing risk assessment models for better financial forecasting
9. Accelerating the discovery of new materials with specific properties
10. Supply chain optimization
11. Optimizing treatment plans
12. Speeding up drug discovery
13. Optimizing the dosage distribution in cancer therapy
14. Optimizing distribution of electricity in smart grids
15. Optimizing extraction efficiency of oil to reduce environmental impact
16. Optimizing battery charging and discharging cycles for efficient usage\
17. Optimizing cargo loading and unloading
18. Optimizing air traffic flow and schedules
19. Optimizing placement of sensors to monitor endangered species
20. Optimizing pollution control
21. Dynamic Pricing for businesses
22. Hyperparameter tuning in Machine Learning
23. Optimization of Cryptographic algorithms
24. Enhancing network intrusion detection systems
25. Waste management cycle optimization
26. Optimizing water distribution networks.

Figure 14. Brainstorming and Ideation

3.2.1 Best idea

Final 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

3.2.2 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

Chapter 4: Prototyping

4.1 Preamble: Introduction to Prototyping

Prototyping is an essential part of the Design Thinking process. It is the culmination of all the techniques and ideas that have been implemented so far. Prototyping refers to testing the ideas that we came up with during the ideation, and making quick changes to cater to our customers.

Prototyping employs a set of tools and approaches for testing out ideas before putting in actual resources, time and effort. It’s like a mock-up of the final product that one intends to put out in the market. It’s a sample experiment of a proposed solution, for testing and validation of ideas. It usually refers to bringing the ideas to life and exploring their impact in the real world, before their final execution. Regardless of how well a person has researched a particular idea, without studying the real life implications of the proposed idea, there is always scope for improvement, and testing is crucial to the success of the design thinking process.

Prototyping helps in clearing out assumptions and biases that a person may have about their proposed solution. Sometimes the developer may become too fixated on the ideas generated during the ideation phase, without considering the negatives and disadvantages of the same on their customer base. Therefore prototyping is essential, as it assesses the product from the point of view of the consumer, without exhausting resources for the same. It can be quick and rough, or well elaborated and thought out, depending on the stage of prototype development.

4.2 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:

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

- 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

4.2.2 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.

4.2.3 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.

4.2.4 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.

4.3 Prototyping implementation details

4.3.1 Libraries used

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

4.3.2 Huffman encoding

- Each bit of the Huffman-encoded stream is mapped to a quantum state: $0 \rightarrow |0\rangle$ and $1 \rightarrow |1\rangle$
- 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.

4.3.3 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.

4.3.4 Flow of encryption

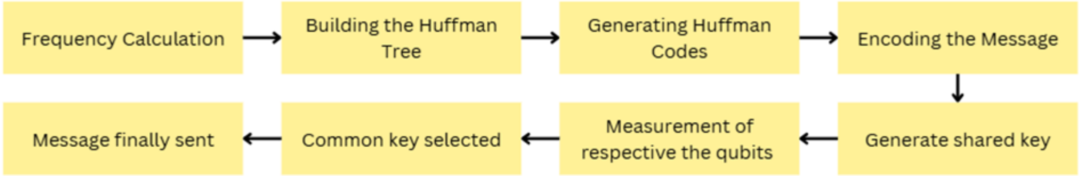


Figure 15: Method of encryption

4.3.5 Flow of decryption

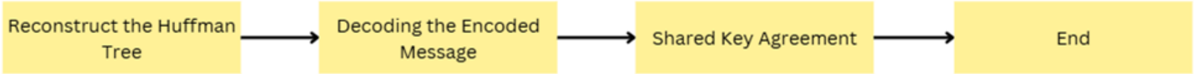


Figure 16: Method of decryption

4.4 Source Code of the Prototype

```
import json
import heapq
from collections import defaultdict
from flask import Flask, request, jsonify, render_template
import pennylane as qml
import numpy as np
import random as r

app = Flask(__name__)

# PennyLane QKD setup
dev = qml.device("default.qubit", wires=2)

@qml.qnode(dev)
def qkd_circuit():
    qml.Hadamard(wires=0)  # Alice applies Hadamard gate
    qml.CNOT(wires=[0, 1])  # Entangle Alice's and Bob's qubits
    return qml.probs(wires=[0, 1])  # Measure the qubits

def simulate_qkd(message_length):
    alice_bases = np.random.randint(0, 2, message_length)  # Alice's
bases (0 or 1)
    bob_bases = np.random.randint(0, 2, message_length)    # Bob's
bases (0 or 1)

    measurement_probs = qkd_circuit()

    shared_key = []
    for i in range(message_length):
        if alice_bases[i] == bob_bases[i]:
            shared_key.append(int(measurement_probs[alice_bases[i]] >
0.5))

    return alice_bases.tolist(), bob_bases.tolist(), shared_key

# Node definition for Huffman tree
class Node:
    def __init__(self, char, freq):
        self.char = char
        self.freq = freq
        self.left = None
        self.right = None

    def __lt__(self, other):
        return self.freq < other.freq
```

```
    def to_dict(self):
        return {
            'char': self.char,
            'freq': self.freq,
            'left': self.left.to_dict() if self.left else None,
            'right': self.right.to_dict() if self.right else None
        }

    @staticmethod
    def from_dict(data):
        node = Node(data['char'], data['freq'])
        if data['left']:
            node.left = Node.from_dict(data['left'])
        if data['right']:
            node.right = Node.from_dict(data['right'])
        return node

def generate_huffman_codes(node, prefix="", codebook=None):
    if codebook is None:
        codebook = {}
    if node is not None:
        if node.char is not None:
            codebook[node.char] = prefix
        generate_huffman_codes(node.left, prefix + "0", codebook)
        generate_huffman_codes(node.right, prefix + "1", codebook)
    return codebook

def huffman_encode(text, codebook):
    return ''.join(codebook[char] for char in text)

def huffman_decode(encoded_text, root):
    decoded_text = []
    node = root
    for bit in encoded_text:
        node = node.left if bit == "0" else node.right
        if node.char is not None:
            decoded_text.append(node.char)
            node = root
    return ''.join(decoded_text)

def build_huffman_tree_from_dict(data):
    return Node.from_dict(data)

@app.route('/')
def index():
    return render_template('index.html')
```

```
@app.route('/alice/chat', methods=['POST'])
def alice_chat():
    data = request.get_json()
    message = data.get("message")

    if not message:
        return jsonify({"error": "No message provided"}), 400

    # Huffman encoding the message
    freq = defaultdict(int)
    for char in message:
        freq[char] += 1
    print(char, freq)
    priority_queue = [Node(char, freq) for char, freq in freq.items()]
    heapq.heapify(priority_queue)

    while len(priority_queue) > 1:
        left = heapq.heappop(priority_queue)
        right = heapq.heappop(priority_queue)
        merged = Node(None, left.freq + right.freq)
        merged.left = left
        merged.right = right
        heapq.heappush(priority_queue, merged)

    huffman_tree_root = priority_queue[0]
    codebook = generate_huffman_codes(huffman_tree_root)
    encoded_message = huffman_encode(message, codebook)

    # Simulate QKD using PennyLane
    alice_bases, bob_bases, shared_key = simulate_qkd(len(message))

    data_to_send = {
        'message': message,
        'encoded_message': encoded_message,
        'alice_bases': alice_bases,
        'bob_bases': bob_bases,
        'shared_key': [r.choice([0, 1]) for _ in range(8)],
        'huffman_tree_root': huffman_tree_root.to_dict(),
    }

    # Save message for Bob to receive
    with open('message_from_alice.json', 'w') as f:
        json.dump(data_to_send, f)

    # Respond back to Alice with the same message
    return jsonify({
        "status": "Message sent to Terminal B",
        "encoded_message": encoded_message,
```

```
        "decoded_message": huffman_decode(encoded_message,
huffman_tree_root),
        "shared_key": ''.join(map(str, shared_key))
    })

@app.route('/bob/chat', methods=['POST'])
def bob_chat():
    data = request.get_json()
    message = data.get("message")

    if not message:
        return jsonify({"error": "No message provided"}), 400

    # Huffman encoding the message
    freq = defaultdict(int)
    for char in message:
        freq[char] += 1

    priority_queue = [Node(char, freq) for char, freq in freq.items()]
    heapq.heapify(priority_queue)

    while len(priority_queue) > 1:
        left = heapq.heappop(priority_queue)
        right = heapq.heappop(priority_queue)
        merged = Node(None, left.freq + right.freq)
        merged.left = left
        merged.right = right
        heapq.heappush(priority_queue, merged)

    huffman_tree_root = priority_queue[0]
    codebook = generate_huffman_codes(huffman_tree_root)
    encoded_message = huffman_encode(message, codebook)

    # Simulate QKD using PennyLane
    bob_bases, alice_bases, shared_key = simulate_qkd(len(message))

    data_to_send = {
        'message': message,
        'encoded_message': encoded_message,
        'alice_bases': alice_bases,
        'bob_bases': bob_bases,
        'shared_key': [r.choice([0, 1]) for _ in range(8)],
        'huffman_tree_root': huffman_tree_root.to_dict(),
    }

    # Save message for Bob to receive
    with open('message_from_bob.json', 'w') as f:
        json.dump(data_to_send, f)
```

```
    # Respond back to Alice with the same message
    return jsonify({
        "status": "Message sent to Terminal A",
        "encoded_message": encoded_message,
        "decoded_message": huffman_decode(encoded_message,
huffman_tree_root),
        "shared_key": ''.join(map(str, shared_key))
    })

@app.route('/alice/receive', methods=['POST'])
def alice_receive():
    # Read Bob's message from the file
    try:
        with open('message_from_bob.json', 'r') as f:
            data = json.load(f)
    except FileNotFoundError:
        return jsonify({"error": "No message found from Bob"}), 404

    huffman_tree_root =
build_huffman_tree_from_dict(data['huffman_tree_root'])
    encoded_message = data['encoded_message']
    decoded_message = huffman_decode(encoded_message,
huffman_tree_root)

    shared_key = [r.choice([0, 1]) for _ in range(8)]
    original_message = data['message']

    return jsonify({
        "decoded_message": decoded_message,
        "shared_key": ''.join(map(str, shared_key)),
        "original_message": original_message
    })

@app.route('/bob/receive', methods=['POST'])
def bob_receive():
    # Read Bob's message from the file
    try:
        with open('message_from_alice.json', 'r') as f:
            data = json.load(f)
    except FileNotFoundError:
        return jsonify({"error": "No message found from Bob"}), 404

    huffman_tree_root =
build_huffman_tree_from_dict(data['huffman_tree_root'])
    encoded_message = data['encoded_message']
    decoded_message = huffman_decode(encoded_message,
huffman_tree_root)
```

```
    shared_key = [r.choice([0, 1]) for _ in range(8)]
    original_message = data['message']

    return jsonify({
        "decoded_message": decoded_message,
        "shared_key": ''.join(map(str, shared_key)),
        "original_message": original_message
    })


if __name__ == '__main__':
    app.run(debug=True, host='0.0.0.0')
```

4.5 Working of the prototype

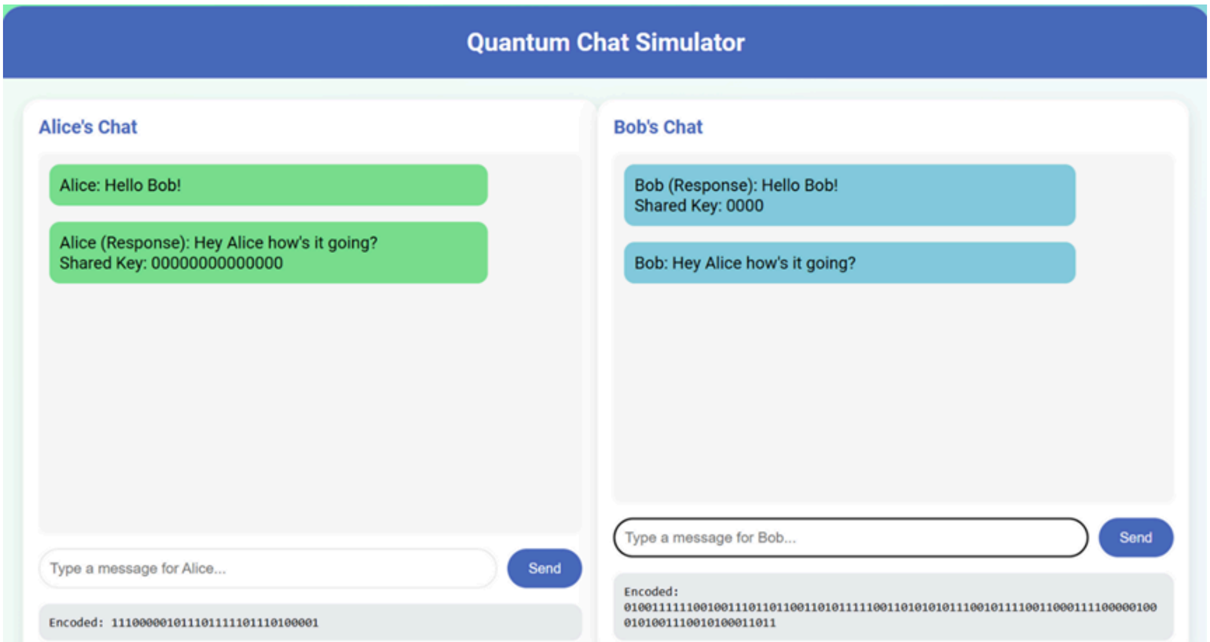


Figure 17: Image of the prototype

4.5.1 Google Colab Notebook representing the Data-transmission and security

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.

4.5.2 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.

Chapter 5: Testing

5.1 Introduction to testing

Testing refers to generation of feedback from the user, for the prototype developed, to gain a deeper understanding of the users. It can be combined with prototyping or taken up as a different stage of design thinking. When undertaken correctly, the testing stage of the project can often feed into most stages of the Design Thinking process: it allows you to Empathise and gain a better understanding of your users; it may lead to insights that change the way you Define your problem statement; it may generate new ideas in the Ideation stage; and finally, it might lead to an iteration of the Prototype.

5.1.1 Types of testing done

Initially, we sent out surveys to our customers, asking them for their feedback on the ideas that we had come up with. Based on the feedback received, we updated our idea, and asked for their feedback again. This was done to ensure that the customers know how valuable their input is for us, and to cater to the needs of our stakeholders.

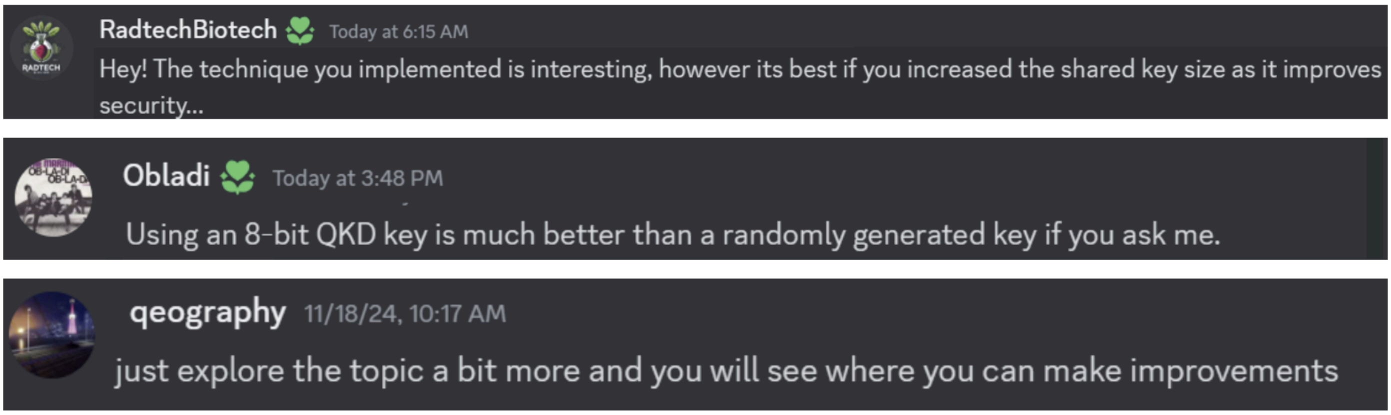


Figure 18. Customer Feedback

It was then 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.

5.2 Validation

5.2.1 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.

5.3 Changes/Modifications

5.3.1 The Adjusted Prototype

Some of the changes incorporated by us on acquiring the feedback from our stakeholders

5.4 Future Scope

- **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.

Chapter 6: Conclusion and Reflection

6.1 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.

6.2 Reflection

Inspiring creative confidence is the number one aim of Design Thinking. Unlike sitting in classrooms and just imbibing information, it is vital to apply it in our daily world to produce a tangible change. In Spite of having abundant knowledge, it becomes very clear in the beginning of the journey that application can be a cumbersome process. What we learnt in Design Thinking not only serves as a benchmark for further projects but is also a vital component of personality development. Observing the nuances of this course we realize that it helps us evolve into well spoken, clear minded and team oriented individuals. Not only is this a medium for hands-on knowledge gaining, but is a reminder to us of the very essence of the word “Engineers”. What else are we studying, if not to help and return to our community.

Unlike scientists who discover or clerks who do mundane work, engineers have a very special role. It is to find solutions to problems. This course sharpens this very critical thinking skill and helps us hone and master the logic analyzation aspect. By engaging with the complete design thinking process, we not only had a chance to learn by doing, but we also came to better understand the value of rapid prototyping, eliciting needs and empathizing by listening closely to my partner throughout each stage of the process. Rapid prototyping, exacerbated by the time constraints, helped me to generate many ideas, and to see how we could engage my “user” as a collaborator in the building process.

Reflecting on our three month journey, it becomes clear that not only did our idea of our idea change, but also the very notion of what we were trying to achieve had been altered for the better. We come to realize that Design Thinking is extremely useful in tackling problems that are ill-defined or unknown, by re-framing the problem in human-centric ways, creating many ideas in brainstorming sessions, and adopting a hands-on approach in prototyping and testing.

Bibliography

[1] *5 Stages in the Design Thinking Process* by Rikke Friis Dam and Teo Yu Siang, Interaction Design Foundation.

[2] *Design Thinking: Getting Started with Empathy* by Rikke Friis Dam and Teo Yu Siang, Interaction Design Foundation.

[3] *Stage 1 in the Design Thinking Process: Empathise with Your Users* by Ditte Hvas Mortensen.

[4] *Stage 3 in the Design Thinking Process: Ideate* by Rikke Friis Dam and Teo Yu Siang, Interaction Design Foundation.

[5] *Stage 4 in the Design Thinking Process: Prototype* by Rikke Friis Dam and Teo Yu Siang

[6] Ashish Kapoor and Rosalind W. Picard, *Multimodal Affect Recognition in Learning Environments*, MIT Media Laboratory, Cambridge, MA 02139, USA