

Infraestrutura Óptica para Comunicação Quântica: Planejamento e Otimização

Karcius D. R. Assis¹

¹Escola Politécnica – Universidade Federal da Bahia (UFBA)
Rua Prof. Aristides Novis nº 02 Federação – CEP: 40210-630 – Salvador – BA – Brasil

karcius.assis@ufba.br

Abstract. This paper proposes an optimization model for Quantum Communication Infrastructure (QCI) to minimize capital expenditure (CAPEX) related to quantum links and trusted repeater nodes. Using Integer Linear Programming (ILP), the model optimizes resource allocation under physical and operational constraints. Simulations in AMPL/CPLEX demonstrate significant CAPEX reductions with increased wavelength availability, achieving optimal or near-optimal cost efficiency. Results validate the model's applicability for medium-scale and efficient QCI deployment in practical scenarios.

Resumo. Este artigo propõe um modelo de otimização para Infraestruturas de Comunicação Quântica (QCI), visando minimizar os custos de capital (CAPEX) associados a links quânticos e nós repetidores confiáveis. Utilizando Programação Linear Inteira (ILP), o modelo otimiza a alocação de recursos sob restrições físicas e operacionais. Simulações realizadas no ambiente AMPL/CPLEX demonstram reduções significativas no CAPEX com o aumento da disponibilidade de comprimentos de onda, alcançando uma relação custo-eficiência ótima ou próxima da ótima. Os resultados validam a aplicabilidade do modelo para a implantação em redes de média escala e eficiência de QCIs em cenários práticos.

1. Introdução

Estamos vivendo uma nova era da computação quântica, na qual processadores quânticos com centenas e até milhares de bits quânticos (qubits) já estão em operação, desafiando os limites da computação clássica [Fedorov et al. 2022]. Esses processadores são compostos por sistemas quânticos meticulosamente projetados e controlados para resolver problemas intratáveis até mesmo pelos supercomputadores clássicos mais poderosos [Boixo et al. 2014, Pokharel and Lidar 2023].

Apesar dos avanços tecnológicos significativos, esses dispositivos ainda enfrentam limitações em sua operação devido à presença de ruídos, os quais reduzem a coerência quântica e introduzem erros nos cálculos. De fato, a presença de erros é um dos maiores desafios da computação quântica. No entanto, recentemente, um marco significativo foi alcançado na construção de processadores quânticos tolerantes a falhas com a Google Quantum AI (<https://quantumai.google/>). Em dezembro de 2024, foi lançado um chip quântico que incorpora métodos eficientes de correção de erros, permitindo que esses processadores se tornem exponencialmente mais precisos à medida que o número de

qubits aumenta [Neven 2025]. Este mesmo processador, denominado Willow, também demonstrou um desempenho sem precedentes, realizando um cálculo de benchmark padrão em menos de cinco minutos, um cálculo que, em um dos supercomputadores mais rápidos atualmente, levaria 1025 anos para ser concluído [AI et al. 2023].

A demonstração do desempenho sem precedentes do processador Willow não apenas sublinha o avanço significativo na computação quântica, mas também abre novas possibilidades para a comunicação quântica. A comunicação quântica oferece potencial para transformar a segurança e a eficiência das redes de comunicação, [Le and Nguyen 2022, Abreu et al. 2024]. Ao utilizar fenômenos como o emaranhamento quântico e a criptografia quântica, é possível criar sistemas de comunicação imunes a interceptações, o que torna a comunicação quântica uma área promissora, especialmente para aplicações em segurança cibernética. O avanço na capacidade de processamento quântico, como demonstrado pelo Willow, pode, em um futuro próximo, integrar-se de forma vital com redes de comunicação quântica, que são formadas também por nós quânticos (processadores quânticos).

Logo, a comunicação quântica representa uma revolução nos paradigmas de transmissão e segurança de dados, oferecendo novas possibilidades para proteger informações sensíveis em aplicações como *e-banking*, *e-health* e comunicações governamentais, [Kong et al. 2023]. Um dos pilares dessa tecnologia é a Distribuição de Chaves Quânticas (*Quantum Key Distribution - QKD*) [Patel et al. 2012], que utiliza princípios da mecânica quântica, como o teorema da não-clonagem, para garantir a inviolabilidade da troca de chaves simétricas entre dois nós de uma rede.

Para implementar uma Infraestrutura de Comunicação Quântica (*Quantum Communication Infrastructure - QCI*), é essencial utilizar links quânticos e nós confiáveis, como os *Trusted Repeater Nodes* (TRNs), [Maity et al. 2024]. No entanto, os custos associados à implantação dessa infraestrutura – conhecidos como CAPEX – são elevados, principalmente devido ao grande número de fibras ópticas e equipamentos especializados necessários para atender às demandas crescentes de segurança. Além disso, a coexistência de sinais quânticos e clássicos em redes multiplexadas por comprimentos de onda *Wavelength Division Multiplexing* (WDM) [Ramaswami et al. 2009]; apresenta desafios técnicos, incluindo a interferência dos sinais clássicos e a degradação das taxas de chave secreta (*secret key rate - SKR*) em longas distâncias.

Neste contexto, a otimização dos recursos da rede torna-se crucial para viabilizar a implantação prática de QCIs. Abordagens baseadas em técnicas de otimização, como a Programação Linear Inteira (*Integer Linear Programming - ILP*) [Maity et al. 2024, Wenning et al. 2023, Cao et al. 2019], têm-se mostrado eficazes na minimização do CAPEX, garantindo que todos os nós quânticos estejam conectados com o menor número de links e TRNs possível. Esses modelos permitem considerar múltiplos aspectos da infraestrutura óptica para reduzir os custos de capital sem comprometer o desempenho da rede.

Este trabalho apresenta uma abordagem para o planejamento e otimização de QCIs, utilizando uma formulação ILP para minimizar o CAPEX enquanto atende às demandas de QKD sob restrições físicas. O trabalho é inspirado na formulação matemática de [Maity et al. 2024]. Entretanto, nós consideramos restrições adicionais, as quais for-

mam um sistema WDM, o qual pode tornar o projeto mais flexível.

Simulações realizadas no ambiente AMPL/CPLEX [IBM 2023] demonstram a eficiência do modelo em cenários com diferentes números de comprimentos de onda disponíveis. Os resultados obtidos destacam o impacto direto da variação de comprimentos de onda no custo de implantação, fornecendo subsídios fundamentais para o planejamento de redes quânticas que sejam, ao mesmo tempo, eficientes, viáveis economicamente e escaláveis.

1.1. Contribuições

As principais contribuições deste trabalho podem ser resumidas da seguinte forma:

- **Proposição de uma formulação matemática robusta:** Desenvolvemos um modelo baseado em ILP que minimiza o CAPEX ao otimizar a utilização de links quânticos, nós e comprimentos de onda em redes quânticas.
- **Consideração do sistema óptico:** O modelo aborda as restrições de interferência e degradação das taxas de chave secreta (SKR) em sistemas multiplexados. Também, avaliamos o impacto de diferentes configurações de disponibilidade de comprimentos de onda na eficiência da infraestrutura, demonstrando a redução de custos e recursos necessários para atender às demandas de QKD.
- **Implementação e validação com software de otimização:** As simulações foram realizadas no ambiente AMPL utilizando o solver CPLEX, garantindo a robustez e a precisão dos resultados obtidos.
- **Aplicabilidade prática:** Demonstramos que a abordagem proposta é escalável e aplicável a topologias de tamanho médio e cenários diferentes, tornando-a uma solução viável para o planejamento de QCI.

1.2. Organização

O restante deste artigo está organizado da seguinte forma: a Seção 2 apresenta os trabalhos relacionados, destacando os avanços e limitações das abordagens existentes; a Seção 3 descreve a metodologia utilizada. Seção 4 detalha a formulação matemática proposta; Seção 5 apresenta os resultados e uma discussão aprofundada sobre a relação entre disponibilidade de comprimentos de onda, o número de links quânticos necessários e o CAPEX, identificando o ponto de equilíbrio ideal para a implantação de redes quânticas. Por fim, a Seção 6 apresenta as conclusões e direções futuras para pesquisas na área.

2. Trabalhos Relacionados

Esta seção apresenta trabalhos recentes sobre o planejamento de redes de comunicação quântica, coexistência clássico-quântica para QKD e orquestração de solicitações QKD.

Algoritmos heurísticos para árvores de cobertura mínima (MST) e árvore de menor caminho com uma única fonte foram propostos por [Gunkel et al. 2019] para conectar todos os nós quânticos (QNs) com a menor estrutura física possível. Contudo, o estudo não examinou a escalabilidade dessas soluções heurísticas em relação ao tamanho da QCI. Também, em relação a planejamento, um algoritmo de agregação de trechos que minimiza o número de TRNs na rede foi proposto por Patri *et al.* [Patri et al. 2023]. Esse método utiliza o limite de transmissão dos QNs para determinar dinamicamente as localizações dos TRNs.

Alguns estudos investigam a coexistência clássico-quântica para QKD. Em tais redes, o ruído gerado pelos sinais clássicos interfere nos sinais quânticos, reduzindo a taxa de chave, especialmente em longas distâncias. Kong *et al.* [Kong et al. 2023] propuseram uma arquitetura de transmissão simultânea para QKD de longa distância e sinais clássicos. Os autores calculam taxas de chave secreta (SKRs) considerando a influência de ruídos provenientes de sinais clássicos. Outro trabalho, em [Patel et al. 2012], demonstra QKD utilizando o efeito de filtragem temporal para abordar o compromisso entre a distância de QKD e SKR. A configuração experimental permite QKD em alta taxa em fibras de até 90 km de comprimento. Em um trabalho relativamente recente, Geng *et al.* [Geng et al. 2021] implementaram QKD em uma rede WDM onde sinais quânticos e clássicos coexistem. O sistema QKD proposto atinge uma SKR de 11 kbps em uma fibra óptica de 20 km de comprimento. Lin *et al.* [Lin and Chen 2021] propuseram uma estratégia de alocação de canais com redução mínima de espalhamento Raman espontâneo (SRS) para acomodar sinais clássicos e quânticos em um sistema WDM denso (DWDM).

Para atender à demanda de taxa de chave das solicitações QKD, Cao *et al.* [Cao et al. 2019] propuseram um algoritmo heurístico para minimizar o custo de implantação de QKD em uma rede WDM. Contudo, apenas redes de alcance limitado podem se beneficiar desse trabalho. Zhang *et al.* [Zhang et al. 2022] maximizam o número de solicitações QKD atendidas considerando o armazenamento de chaves e bypass óptico.

Nosso trabalho é inspirado em [Maity et al. 2024], o qual apresenta uma formulação que minimiza o custo da QCI. Entretanto, nós consideramos um fator essencial na fase do planejamento da QCI, que é a disponibilidade de comprimentos de onda para o projeto da rede quântica. Portanto, neste trabalho, otimizamos iterativamente tanto o custo de implantação da QCI (em termos de fibras utilizadas, aqui chamado CAPEX) quanto as rotas das demandas QKD considerando os efeitos de disponibilidade de comprimentos de onda.

3. Metodologia: Fluxo de Otimização Proposto

O processo de planejamento e otimização da QCI pode ser descrito por meio de um fluxograma que detalha as etapas principais, desde a entrada dos dados da infraestrutura física até a obtenção da solução otimizada (Figura 1). Este fluxo de planejamento é dividido em três componentes principais: entrada, otimização e saída, conforme descrito a seguir.

- Infraestrutura física original (entrada): Consiste na topologia física da rede óptica, representada por links e nós disponíveis, como mostrado na Figura 1. Também comprimentos de onda disponíveis $|C|$, que irão determinar o número de canais quânticos que podem ser alocados em cada link da rede por meio de técnicas de multiplexação (WDM). O valor de $|C|$ é um fator crítico para a eficiência da rede e afeta diretamente o número de links físicos necessários para atender às demandas de QKD, que também são entradas. Taxas de chaves também fazem parte da entrada. Essas informações servem como base para o modelo de otimização.
- A segunda etapa do processo é a resolução do problema ILP ou otimização, que tem como objetivo minimizar o CAPEX da infraestrutura quântica. Nesta etapa a formulação ILP considera os custos de capital associados à instalação de links quânticos e TRNs, além de respeitar restrições operacionais, como limites de atenuação nos links e capacidade de multiplexação.

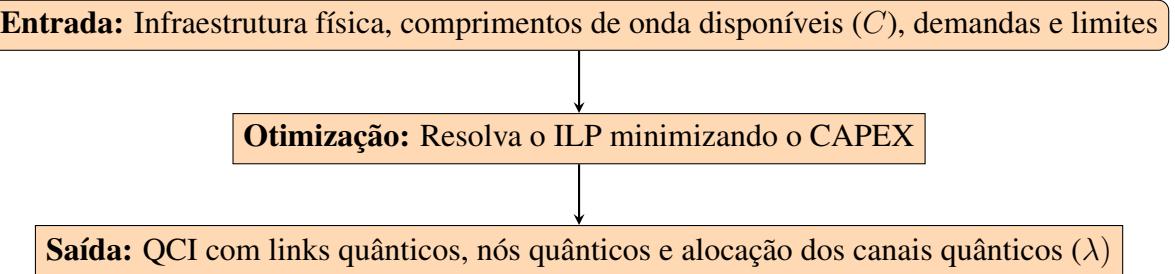


Figura 1. Processo de planejamento e otimização

- A solução (ou saída) do modelo fornece uma QCI otimizada que conecta todos os QNs e links quânticos, mantendo a conectividade da rede e respeitando as restrições. Também há alocação de λ 's (comprimentos de onda disponíveis pertencentes a um conjunto de um total de comprimentos de onda disponíveis) para os canais quânticos, para distribuição eficiente desses canais nos links selecionados, garantindo o atendimento das demandas de QKD.

Este processo garante que a infraestrutura resultante atenda às demandas de segurança quântica de maneira eficiente, com o menor custo possível, ao mesmo tempo em que respeita as limitações práticas da tecnologia óptica e quântica.

4. Formulação do Problema

O objetivo do ILP é implantar uma QCI com custo mínimo, conectando todos os QNs com o menor número de TRNs e atendendo às demandas de QKD. A definição dos parâmetros e variáveis, assim como a formulação matemática, é apresentada a seguir:

Tabela 1. Descrição dos Termos Utilizados na Formulação do Problema

Símbolo	Descrição
Parâmetros:	
F	Conjunto de todas as demandas de QKD.
r_k	Taxa de chave secreta demandada por $f_k \in F$.
r_{ij}	Taxa de chave secreta do link e_{ij} .
E	Conjunto de arestas e_{ij} da topologia física.
W	Límite de atenuação para links quânticos.
C	Conjunto de comprimentos de onda λ , ou seja, $C=\{\lambda_1, \lambda_2... C \}$.
V_T	Conjunto de nós da QCI.
q_s^k	Nó quântico que é fonte.
q_d^k	Nó quântico que é destino.
Variáveis:	
x_{ij}	Variável binária indicando se a aresta e_{ij} pertence à QCI.
y_{ij}^k	Variável binária indicando se a demanda f_k utiliza a aresta e_{ij} .
T_n	Variável que indica a quantidade de repetidores/trusted node em um nó n .

4.1. Modelo ILP

Objetivo

A função objetivo visa minimizar o Custo de Capital (CAPEX), referente à implantação da infraestrutura, os links quânticos e, consequentemente, os QNs.

$$\text{Minimizar} \sum_{e_{ij} \in E} x_{ij}, \quad (1)$$

Restrições

Restrição (2) garante que cada QN, de um link $i - j$, está conectado à infraestrutura mínima QCI. Ou seja, pelo menos uma aresta deve estar conectada à QCI.

$$\sum_{e_{ij} \in E} x_{ij} \geq 1, \quad (2)$$

Restrição (3) limita a atenuação dos links quânticos ao máximo suportado pelos transceptores quânticos. A atenuação do link w_{ij} multiplicado pela variável x_{ij} (indicando se o link é usado ou não) deve ser menor que o limite W .

$$x_{ij}w_{ij} \leq W, \quad \forall e_{ij} \in E, \quad (3)$$

Restrição (4) garante que a soma das taxas de chave secreta r_k das demandas, cada qual no canal quântico λ (comprimento de onda) alocadas em um link e_{ij} não exceda a taxa de chave secreta disponível r_{ij} daquele link.

$$\sum_{f_k \in F, \lambda \in C} y_{ij,\lambda}^k r_k \leq x_{ij}r_{ij}, \quad \forall e_{ij} \in E \quad (4)$$

Restrição (5) garante que os fluxos de dados de QKD sejam balanceados entre a fonte q_s^k e o destino q_d^k .

$$\sum_{q_j \in V_T, \lambda \in C} y_{ij,\lambda}^k - \sum_{q_j \in V_T, \lambda \in C} y_{ji,\lambda}^k = \begin{cases} 1 & \text{se } q_i = q_s^k, \\ -1 & \text{se } q_i = q_d^k, \\ 0 & \text{caso contrário.} \end{cases} \quad \forall f_k \in F, \quad (5)$$

Restrição (6) estabelece que uma demanda de QKD, no comprimento de onda λ , pode ser roteada em uma aresta $i - j$ somente se essa aresta fizer parte da QCI (ou seja, $x_{ij} = 1$)

$$y_{ij,\lambda}^k + y_{ji,\lambda}^k \leq x_{ij}, \quad \forall e_{ij} \in E, \forall f_k \in F, \lambda \in C \quad (6)$$

Restrição (7) garante unicidade de comprimento de onda para cada demanda no link ij .

$$\sum_{f_k \in F} y_{ij,\lambda}^k \leq 1, \quad \forall e_{ij} \in E, \lambda \in C \quad (7)$$

Restrição (8) diz se há repetidores e quantidade (quando houver) em qualquer QN da rede. Ou seja, na configuração da QCI alguns nós podem ser apenas QNs fonte e destino, enquanto outros são QNs repetidores ou *trusted nodes*.

$$\sum_{f_k \in F, e_{i,n} \in E, \lambda \in C} y_{in,\lambda}^k = T_n, \quad \forall i \neq n \neq q_{dest}^k \quad (8)$$

A restrição (9) garante que os canais quânticos de todas as requisições de QKD passando por um link deve ser limitado ao número total de comprimento de onda disponíveis.

$$\sum_{f_k \in F, \lambda \in C} y_{ij,\lambda}^k \leq |C|, \quad \forall e_{i,j} \in E, \quad (9)$$

$$x_{ij}, y_{ij,\lambda}^k \in \{0, 1\}, T_j \in Z \quad \forall e_{ij} \in E, \forall f_k \in F, \forall \lambda \in C. \quad (10)$$

A formulação matemática apresentada nesta seção estabelece uma abordagem para a construção de QCI com custo mínimo. Utilizando o ILP, o modelo busca minimizar o CAPEX ao otimizar a utilização de links quânticos, comprimentos de onda e QNs, enquanto atende às restrições físicas e operacionais da rede.

A função objetivo incorpora uma análise do custo de capital, enquanto as restrições garantem a conectividade da rede e a viabilidade técnica de implementação. O modelo proposto é escalável, permitindo sua aplicação em topologias de tamanho médio e também para uma quantidade razoável de demandas.

A próxima seção apresenta os resultados obtidos a partir de simulações computacionais. Estas simulações ilustram o desempenho da abordagem proposta em diferentes cenários, demonstrando sua eficiência e validando as premissas do modelo matemático.

5. Simulações e Resultados

As simulações foram realizadas no ambiente de otimização AMPL [IBM 2023], com resolução utilizando o solver CPLEX [IBM 2023], devido à sua eficiência em resolver problemas ILP. Nós assumimos que há o protocolo BB84 [Bennett and Brassard 2014] para QKD, um dos protocolos mais amplamente estudados e implementados, devido à sua robustez e simplicidade em contextos práticos.

5.1. Configuração Inicial

Primeiramente, foi utilizada uma rede de 9 nós consistindo de enlaces de fibras interconectados, cada um caracterizado por propriedades específicas:

- **Topologia da Rede:** A topologia física é dada com distância de 100km entre nós. Os nós estão equipados com multiplexadores de comprimentos de onda.

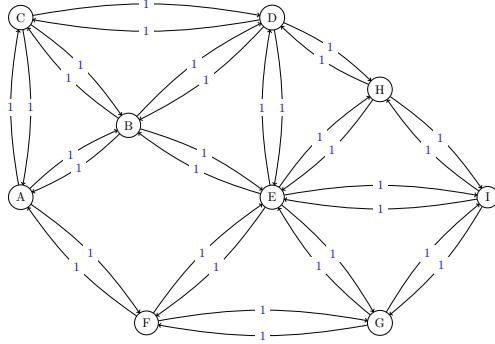


Figura 2. Infraestrutura óptica disponível (topologia física)

- **Requisitos de Distribuição de Chaves:** Canais de comunicação seguros são estabelecidos usando demandas QKD, com taxas de chave de $r_k = 5\text{kb/s}$ entre os nós (A,H), (B,G), (E,B), (G,D) e (I,A); e uma demanda com taxa de chaves de 3 kb/s entre os nós (D,I), (C,F), (F,E) e (H,C).
- **Outros Parâmetros para Simulações:** A máxima taxa de chaves suportada por cada link físico é de $r_{ij} = 12 \text{ Kb/s}$ e o limite máximo de atenuação é $W=100\text{km}$. Como é assumido que cada link tem 100km, todos os links serão candidatos a fazer parte da QCI.

A análise foi conduzida utilizando a formulação ILP apresentada na Seção 3. O objetivo foi minimizar o CAPEX ou criação de uma mínima QCI, considerando os custos de implantação em termos de número de links quânticos e utilização de comprimentos de onda disponíveis, $|C|$. Para tanto, foram simulados diferentes cenários de disponibilidade de λ , variando o mesmo de $|C|=1$ até $|C| \geq 4$, aplicados a uma topologia física de referência, conforme descrito na Figura 2.

A abordagem iterativa, seguindo o fluxograma da Tabela I, permitiu avaliar o planejamento da QCI. A seguir, cada cenário simulado será detalhado, com uma análise do impacto da otimização nos parâmetros de desempenho avaliados.

Na Figura 3a apenas um comprimento de onda está disponível. Isto resulta em uma maior densidade de links quânticos para atender todas as demandas QKD, logo o CAPEX é elevado nesse caso.

Com dois comprimentos de onda disponíveis (Figura 3b), a eficiência aumenta. Há redução no número de links necessários em comparação a $|C|=1$, mas ainda não é otimizado. Este cenário começa a explorar melhor a multiplexação de comprimentos de onda, diminuindo o CAPEX.

Na Figura 3c, com disponibilidade de três comprimentos de onda, há uma otimização significativa em relação ao número de links. A rede começa a atingir um balanço ideal entre custo e complexidade.

Com quatro ou mais comprimentos de onda disponíveis (Figura 3d), a rede atinge maior eficiência. Os links necessários são bastante reduzidos, formando um anel e minimizando o CAPEX. Este cenário mostra o melhor equilíbrio entre custo de implantação e

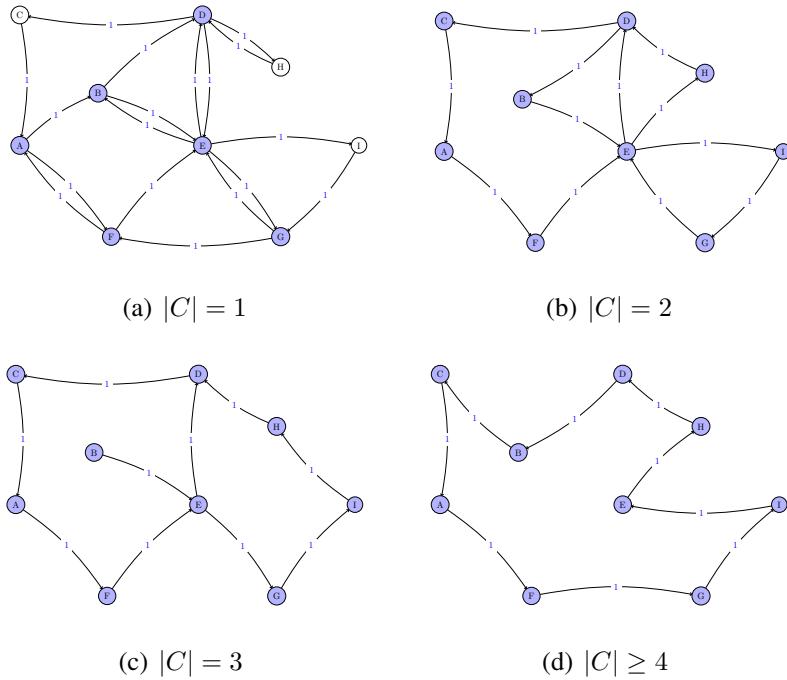


Figura 3. QCI obtida com diferentes números de comprimentos de onda $|\mathcal{C}|$ disponíveis, onde os nós brancos são QNs comuns (apenas usuários finais), e os nós azuis são QNs *trusted nodes* ou repetidores, além de também poderem ser usuários finais.

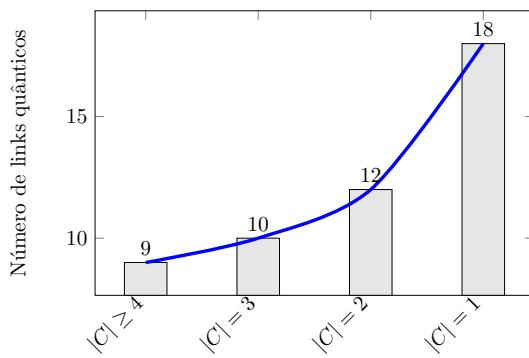


Figura 4. CAPEX (número de links quânticos) em função do número de comprimentos de onda disponíveis $|C|$, rede de 9 nós

utilização de recursos.

A Figura 4 sumariza o resultado das simulações da relação entre $|C|$ e o número de links quânticos necessários para implementar a QCI.

Pode-se notar, que com apenas um comprimento de onda disponível, cada link pode atender apenas uma única demanda. Como resultado, a densidade de links na rede é muito alta.

A disponibilidade de mais comprimentos de onda, por exemplo $|C| = 2$, melhora a otimização, pois permite que múltiplas demandas sejam atendidas por menos links,

reduzindo o CAPEX em cerca de 33% em relação a $|C|=1$.

Com três comprimentos de onda, ocorre uma otimização adicional. A redução no número de links necessários começa a desacelerar, mas ainda é significativa em relação a $|C|=2$ (redução de 16.6%).

Quando $|C|$ atinge ou excede 4, o número de links necessários se estabiliza em 9. Nesse ponto, a capacidade de multiplexação dos comprimentos de onda é suficiente para atender a todas as demandas de maneira eficiente.

5.2. Rede de 20 nós

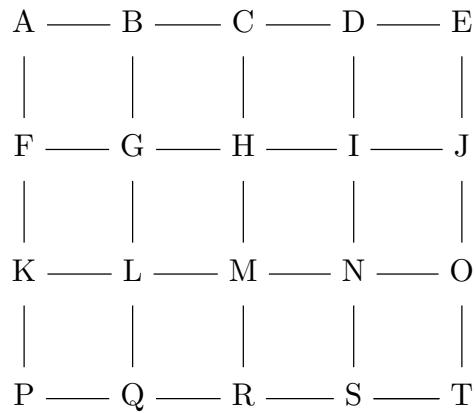


Figura 5. Rede com 20 nós

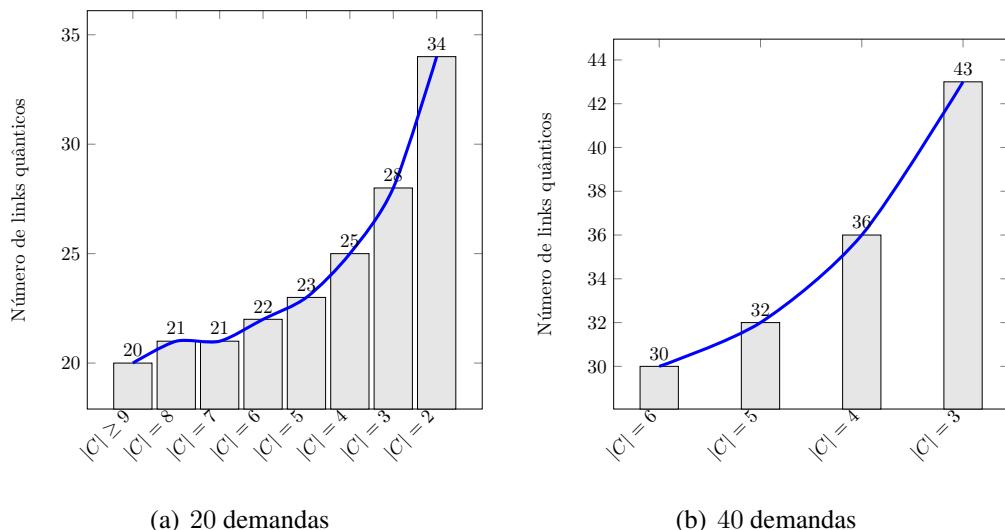


Figura 6. CAPEX em termos do número de comprimentos de onda disponíveis $|C|$ para a rede de 20 nós, (a) 20 demandas e (b) 40 demandas

Também fizemos análises numa rede de 20 nós (Figura 5). Essa configuração, comparada à rede anterior de 9 nós, possui um maior número de links físicos disponíveis

e, consequentemente, maior capacidade de acomodar demandas adicionais. Na análise da Figura 6, os parâmetros físicos permanecem consistentes com os experimentos anteriores, mas as demandas de chave QKD foram geradas aleatoriamente, considerando dois cenários: 20 demandas (Figura 6a) e 40 demandas (Figura 6b).

A rede de 20 nós, devido à sua maior quantidade de links físicos, apresenta uma capacidade superior de lidar com mais demandas, o que permite observar uma maior flexibilidade na alocação de recursos. Apesar disso, o comportamento geral de redução do CAPEX com o aumento de $|C|$ é consistente entre os cenários com 9 e 20 nós, confirmado a robustez do modelo ILP.

No caso de 20 demandas (Figura 6a), o CAPEX varia de 34 links (para $|C|=2$) até 20 links (para $|C| \geq 9$). Esse intervalo demonstra a eficiência crescente do modelo na alocação de recursos conforme mais comprimentos de onda são introduzidos. Para 40 demandas (Figura 6b), os valores de CAPEX são mais elevados, variando de 43 links ($|C|=3$) até 30 links ($|C| = 6$), indicando a necessidade de mais recursos para atender ao dobro de demandas.

5.3. Complexidade Computacional

A complexidade computacional no planejamento e otimização de redes maiores, como a de 20 nós com 40 demandas, aumenta substancialmente devido a diversos fatores inerentes ao problema ILP. Esses fatores, como número de variáveis e restrições, interdependência entre demandas etc., estão relacionados ao tamanho da rede e número de demandas a serem atendidas. A cada nó ou link adicionado à rede, o espaço de busca cresce de forma exponencial. Isso ocorre porque o *solver* cplex precisa explorar todas as possíveis configurações de links e comprimentos de onda para encontrar a solução ótima. O aumento no número de demandas amplifica ainda mais o espaço de busca, pois cada nova demanda cria mais possibilidades de alocação. A Figura 7 mostra o tempo de simulação para a rede de 20 nós, com 40 demandas, num Intel(R) Core(TM) i7-4790 CPU @ 3.60GHz, 32 GB de RAM. Com $|C| = 6$ o tempo de simulação é $\approx 3,8h$ (227.2 min), enquanto que com 20 demandas (barras vermelhas na mesma Figura) o tempo de simulação ficou em torno de 1 min para qualquer valor de $|C|$.

O aumento do tempo de simulação em redes maiores e com várias demandas reflete a natureza combinatória do problema ILP. Para cenários como o da rede de 20 nós com 40 demandas, estratégias para reduzir o tempo de resolução, como heurísticas, aproximações ou decomposição do problema, podem ser necessárias. Embora essas abordagens possam sacrificar a garantia de solução ótima, elas oferecem soluções eficientes em tempo viável, mantendo a qualidade geral do planejamento da rede. Logo, técnicas heurísticas serão objetos de estudos futuros.

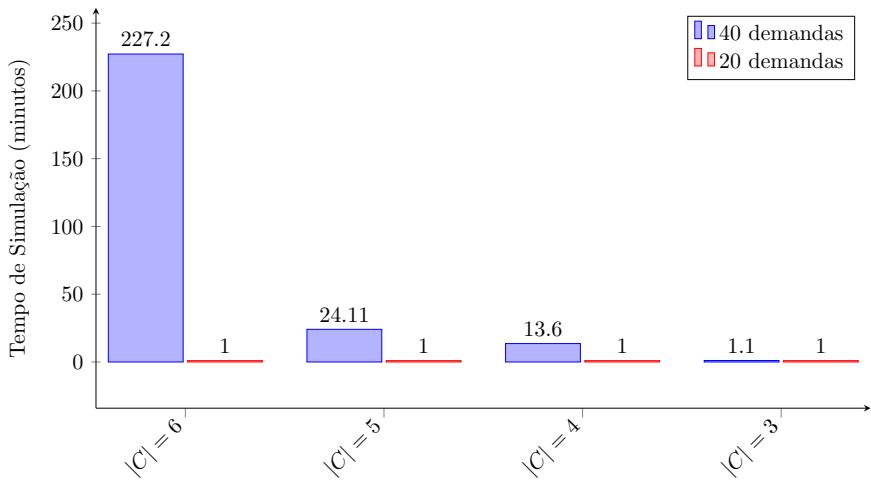


Figura 7. Tempo de Simulação, rede de 20 nós com 40 demandas (barra azul). A barra vermelha mostra o tempo de simulação médio para 20 demandas sobre a mesma rede

6. Conclusão

Este trabalho apresentou uma abordagem inovadora para o planejamento e otimização de QCI, com foco na minimização dos custos de capital por meio da utilização de ILP. Os resultados das simulações destacaram a eficiência do modelo proposto em cenários com diferentes disponibilidades de comprimentos de onda, evidenciando uma relação direta entre o aumento da multiplexação e a redução de custos.

A formulação matemática desenvolvida permitiu atender às demandas de QKD enquanto respeitava as restrições físicas da infraestrutura, demonstrando aplicabilidade prática em topologias de tamanho médio. Além disso, os cenários simulados mostraram que a otimização baseada em ILP é uma ferramenta robusta para projetar QCIs economicamente viáveis e escaláveis, contribuindo para a viabilização prática das comunicações quânticas em larga escala.

Como direções futuras, propõe-se a expansão do modelo para topologias mais complexas e a inclusão de fatores como variabilidade de tráfego e confiabilidade dos componentes. Além disso, estudos sobre a integração de tecnologias emergentes, assim como heurísticas ou metaheurísticas, podem potencializar ainda mais o impacto da abordagem apresentada.

Agradecimentos

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001. Também gostaríamos de agradecer ao Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) pelo apoio.

Referências

- Abreu, D., Rothenberg, C. E., and Abelém, A. (2024). Qml-ids: Quantum machine learning intrusion detection system. In *2024 IEEE Symposium on Computers and Communications (ISCC)*, pages 1–6. IEEE.

- AI, G. Q., , and Collaborators (2023). Suppressing quantum errors by scaling a surface code logical qubit. *Nature*, 614(7949):676–681.
- Bennett, C. H. and Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. *Theoretical computer science*, 560:7–11.
- Boixo, S., Rønnow, T. F., Isakov, S. V., Wang, Z., Wecker, D., Lidar, D. A., Martinis, J. M., and Troyer, M. (2014). Evidence for quantum annealing with more than one hundred qubits. *Nature physics*, 10(3):218–224.
- Cao, Y., Zhao, Y., Wang, J., Yu, X., Ma, Z., and Zhang, J. (2019). Cost-efficient quantum key distribution (qkd) over wdm networks. *Journal of Optical Communications and Networking*, 11(6):285–298.
- Fedorov, A. K., Gisin, N., Belousov, S. M., and Lvovsky, A. I. (2022). Quantum computing at the quantum advantage threshold: a down-to-business review. *arXiv preprint arXiv:2203.17181*.
- Geng, J.-Q., Fan-Yuan, G.-J., Wang, S., Zhang, Q.-F., Hu, Y.-Y., Chen, W., Yin, Z. Q., He, D.-Y., Guo, G.-C., and Han, Z.-F. (2021). Coexistence of quantum key distribution and optical transport network based on standard single-mode fiber at high launch power. *Optics Letters*, 46(11):2573–2576.
- Gunkel, M., Wissel, F., and Poppe, A. (2019). Designing a quantum key distribution network - methodology and challenges. In *Photonic Networks; 20th ITG-Symposium*, pages 1–3. VDE.
- IBM (2023). *IBM ILOG CPLEX Optimization Studio*. IBM Corporation.
- Kong, W., Sun, Y., Gao, Y., and Ji, Y.-F. (2023). Coexistence of quantum key distribution and optical communication with amplifiers over multicore fiber. *Nanophotonics*, 12:1979–1994.
- Le, L. and Nguyen, T. N. (2022). Dqra: Deep quantum routing agent for entanglement routing in quantum networks. *IEEE Transactions on Quantum Engineering*, 3:1–12.
- Lin, R. and Chen, J. (2021). Modeling and minimizing spontaneous raman scattering for qkd secured dwdm networks. *IEEE Communications Letters*, 25(12):3918–3921.
- Maity, I., ur Rehman, J., and Chatzinotas, S. (2024). Taqnet: Traffic-aware minimum-cost quantum communication network planning. *IEEE Transactions on Quantum Engineering*.
- Neven, H. (2025). Meet willow, our state-of-the-art quantum chip: <https://blog.google/technology/research/google-willow-quantum-chip/>. Acessado em: 20 jan. 2025.
- Patel, K. A., Dynes, J. F., Choi, I., Sharpe, A. W., Dixon, A. R., Yuan, Z. L., Penty, R. V., and Shields, A. J. (2012). Coexistence of high-bit-rate quantum key distribution and data on optical fiber. *Physical Review X*, 2:041010.
- Patri, S. K., Wenning, M., Gonde, S. H., Autenrieth, A., Elbers, J.-P., and Mas-Machuca, C. (2023). Trusted node deployment strategies for long-haul quantum key distribution networks. In *International Conference on Optical Network Design and Modeling (ONDM)*, pages 1–6.

- Pokharel, B. and Lidar, D. A. (2023). Demonstration of algorithmic quantum speedup. *Physical Review Letters*, 130(21):210602.
- Ramaswami, R., Sivarajan, K., and Sasaki, G. (2009). *Optical networks: a practical perspective*. Morgan Kaufmann.
- Wenning, M., Samonaki, M., Patri, S. K., Fehenberger, T., and Mas-Machuca, C. (2023). Multi-layer optimization for qkd and key management networks. *Journal of Optical Communications and Networking*, 15(11):938–947.
- Zhang, Q., Ayoub, O., Gatto, A., Wu, J., Lin, X., Musumeci, F., Verticale, G., and Tornatore, M. (2022). Joint routing, channel, and key-rate assignment for resource-efficient qkd networking. In *IEEE Global Communications Conference (GLOBECOM)*, pages 3676–3681.