

Design-QKD: Software para Planejamento e Análise de Redes QKD sobre uma Infraestrutura Óptica

Jaidan Lessa Oliveira, Alex Ferreira dos Santos e Karcus Day Rosario Assis

Resumo— Este artigo apresenta uma plataforma de simulação para o planejamento de redes de Distribuição de Chaves Quânticas (QKD) sobre infraestruturas ópticas WDM. O software integra visualização de topologias, avaliação de desempenho e heurísticas de otimização para analisar alocação de recursos, posicionamento de nós confiáveis e uso espectral sob restrições operacionais. As simulações permitem explorar trade-offs entre topologia, disponibilidade espectral e custo de implantação. Os resultados indicam que a ferramenta apoia a tomada de decisões e facilita a compreensão de diferentes estratégias de implantação. A plataforma se mostra acessível e adequada para estudos em escala média, contribuindo para pesquisas em redes quânticas.

Palavras-Chave— Redes Quânticas, Distribuição de Chaves Quânticas (QKD), Heurísticas.

Abstract— This article presents a simulation platform for planning Quantum Key Distribution (QKD) networks over WDM optical infrastructures. The software integrates topology visualization, performance evaluation, and heuristic optimization to analyze resource allocation, trusted-node placement, and spectral usage under operational constraints. Simulations allow users to explore trade-offs among topology, spectral availability, and deployment cost. Results show that the tool supports decision-making and enhances understanding of different QKD deployment strategies. The platform is accessible and suitable for medium-scale studies, contributing to research in quantum network planning.

Keywords— Quantum Networks, Quantum Key Distribution (QKD), Heuristics.

I. INTRODUÇÃO

Estamos vivendo uma nova era da computação quântica, marcada pela operação de processadores com centenas ou milhares de qubits, capazes de desafiar os limites da computação clássica [1]. Esses dispositivos, embora promissores para resolver problemas intratáveis por supercomputadores convencionais [2], ainda enfrentam restrições causadas por ruídos quânticos, que comprometem a coerência e introduzem erros. Ainda assim, avanços recentes em correção de erros vêm tornando esses sistemas mais robustos. Um exemplo é o processador *Willow*, anunciado pela Google Quantum AI em dezembro de 2024, que demonstrou métodos eficientes de tolerância a falhas e executou um *benchmark* padrão em menos de cinco minutos, desempenho que supercomputadores clássicos levariam um tempo inviável para reproduzir [3]. Esse progresso na computação quântica também impulsiona avanços na comunicação quântica, área com potencial para transformar a segurança e a eficiência das redes ao explorar fenômenos como emaranhamento e criptografia quântica [4].

Jaidan Lessa Oliveira, Universidade Estadual de Feira de Santana (UEFS). Alex Ferreira dos Santos, Universidade Estadual de Feira de Santana (UEFS) e Universidade Federal do Recôncavo da Bahia (UFRB). Karcus Day Rosario Assis, Universidade Federal da Bahia (UFBA). E-mails para contato: jaidanlessa@gmail.com, alex.ferreira@ufrb.edu.br, karcus.assis@ufba.br.

Nesse contexto, ganha destaque a Infraestrutura de Comunicação Quântica (*Quantum Communication Infrastructure* – QCI), composta por nós quânticos e enlaces capazes de suportar aplicações críticas, como *e-banking*, *e-health* e comunicações governamentais [5].

Entre as principais tecnologias de QCI está a Distribuição de Chaves Quânticas (*Quantum Key Distribution* – QKD) [6], que utiliza princípios da mecânica quântica, como o teorema da não-clonagem, para assegurar a troca segura de chaves simétricas. A implementação prática dessas redes exige enlaces quânticos, nós confiáveis e, em muitos casos, *Trusted Repeater Nodes* (TRNs) [7], além de considerar a coexistência entre tráfego clássico e quântico em sistemas WDM (*Wavelength Division Multiplexing*) [8].

Entretanto, a implantação de QCIs envolve custos elevados de infraestrutura e equipamentos especializados, além de limitações físicas que afetam métricas como a *secret key rate* (SKR). Por isso, a otimização de recursos é fundamental para viabilizar o planejamento dessas redes. Nesse sentido, formulações de Programação Linear Inteira (*Integer Linear Programming* – ILP) vêm sendo empregadas para minimizar CAPEX e apoiar decisões sobre alocação de recursos e posicionamento de TRNs [7, 9].

Apesar desses avanços, ainda há carência de simuladores acessíveis que permitam visualizar e compreender, de forma prática, os desafios envolvidos no planejamento de QCIs. À medida que essas tecnologias se aproximam da adoção real, torna-se importante disponibilizar plataformas que auxiliem pesquisadores e profissionais na análise de cenários, exploração de *trade-offs* e comparação de estratégias de implantação. Motivado por essa lacuna, este trabalho apresenta um simulador para planejamento de redes QKD sobre infraestruturas ópticas multiplexadas em comprimento de onda (QKD-over-WDM). A ferramenta integra visualização de topologias, avaliação de desempenho e heurísticas de otimização para análise de alocação de recursos ópticos e quânticos, incluindo posicionamento de TRNs, utilização espectral e dimensionamento de canais WDM sob restrições físicas e operacionais. Inspirado na formulação ILP de [7], o simulador incorpora restrições adicionais do ambiente óptico multiplexado e permite investigar o impacto da disponibilidade espectral no custo de implantação, oferecendo suporte a estudos de cenários de média escala e ao entendimento de estratégias de implantação de redes quânticas.

As principais contribuições deste trabalho são o desenvolvimento de uma plataforma Web interativa e bilíngue (português/inglês) para planejamento e análise de redes QKD sobre infraestruturas ópticas WDM, que permite a construção gráfica de topologias e configuração dinâmica de parâmetros de simulação, chamada Design-QKD, disponível em <https://designedu-qkd.com/>. Além disso, a ferramenta incor-

pora heurísticas de roteamento clássico e ponderado por SKR, bem como mecanismos automáticos para cálculo de recursos, incluindo TRNs, transceptores e canais WDM, possibilitando análise rápida de *trade-offs* de CAPEX. A plataforma também integra matrizes editáveis de SKR, demanda e distância de transmissão, associadas a visualizações gráficas e matriciais que auxiliam na identificação de gargalos e na análise da utilização de recursos da rede.

O restante deste artigo está organizado da seguinte forma. A Seção II apresenta os trabalhos relacionados. A Seção III descreve a metodologia e o funcionamento da plataforma proposta. A Seção IV apresenta as simulações realizadas e os resultados obtidos. Por fim, a Seção V apresenta as conclusões do trabalho.

II. TRABALHOS RELACIONADOS E COMPARATIVO DE SIMULADORES DE REDES QUÂNTICAS

A literatura recente sobre QCI tem se concentrado predominantemente em dois pilares: a fidelidade física dos protocolos e a otimização matemática de infraestruturas. No entanto, há uma lacuna persistente em ferramentas que integrem essas frentes de forma acessível e visual para o planejamento prático de redes quânticas sobre infraestruturas ópticas.

Estudos focados em otimização, como o de Maity *et al.* (2024) e Cao *et al.* (2019), propõem modelos robustos baseados em ILP para posicionamento ótimo de TRNs e alocação espectral em sistemas WDM, considerando rigorosas restrições de distância e SKR dos enlaces.

Mais recentemente, Ribeiro *et al.* (2025) investigaram o impacto do particionamento de taxa de chave em caminhos disjuntos, demonstrando que essa estratégia aumenta significativamente a robustez contra espionagem, embora eleve o CAPEX em aproximadamente 22,4% [10]. Esses modelos matemáticos são eficientes para otimização global, mas exigem conhecimento avançado de otimização e carecem de interfaces visuais interativas para experimentação rápida por pesquisadores não-especialistas. O Design-QKD incorpora essas abordagens heurísticas, permitindo que o usuário visualize interativamente os *trade-offs* em quantidade e posicionamento de recursos (TRNs, transceptores e canais WDM) em cenários reais de Redes QKD sobre uma Infraestrutura Óptica.

Diversos simuladores de tecnologias quânticas foram desenvolvidos nas últimas décadas, priorizando principalmente a modelagem física de protocolos e ruídos. O NetSquid [11] destaca-se pela modelagem detalhada de estados quânticos, ruído e distribuição de emaranhamento, porém apresenta interface limitada e praticamente inexistente suporte ao planejamento de recursos da Infraestrutura (TRNs, transceptores e alocação WDM). O SeQUeNCe [12] oferece uma arquitetura *full-stack* mais completa, com suporte e gerenciamento de recursos, mas ainda exige curva de aprendizado elevada e não fornece Visualizações intuitivas de *trade-offs* ou matrizes editáveis de distância/SKR/demanda. Ferramentas de alto nível como QuNetSim [13] focam em protocolos simples e integração rápida, assumindo *links* quase ideais, enquanto o QKDNetSim [14] é voltado para a integração QKD com redes clássicas, porém com visualização e análise de alocação espec-

tral bastante limitadas. A Tabela I resume essas características e compara os simuladores com o Design-QKD.

TABELA I
COMPARAÇÃO ENTRE SIMULADORES DE REDES QUÂNTICAS E QKD.

Ferramenta	Foco	Física	Visualização	Recursos
NetSquid	Protocolos e física	Alta	Limitada	Baixa
SeQUeNCe	Redes full-stack	Alta	Moderada	Moderada
QuNetSim	Protocolos simples	Média	Baixa	Baixa
QKDNetSim	Integração QKD	Média	Baixa	Moderada
Design-QKD	Planejamento	Baixa	Alta	Alta

A. Diferenciais de Modelagem Iterativa

Diferentemente dos simuladores citados, que priorizam modelagem física detalhada ou integração de protocolos, o Design-QKD preenche uma lacuna importante ao oferecer uma plataforma Web acessível, multilíngue e voltada especificamente para o planejamento prático. A ferramenta permite a construção gráfica de topologias, o uso de matrizes editáveis de distância máxima de transmissão (por enlace), SKR (por enlace) e demanda (por requisição) e visualizações claras de alocação de recursos (WDM, transceptores e TRNs).

Essa abordagem possibilita modelar cenários realistas em que a qualidade física dos enlaces pode variar individualmente e as demandas de tráfego podem ser heterogêneas entre os nós, facilitando o aprendizado sobre dimensionamento de QCIs e a exploração interativa de *trade-offs* em quantidade e posicionamento de equipamentos. Dessa forma, o Design-QKD se posiciona como uma ferramenta complementar aos simuladores existentes, ideal para estudos preliminares de implementação de redes quânticas em escala média.

III. METODOLOGIA: FLUXO DE OTIMIZAÇÃO DA PLATAFORMA

O Fluxograma 1 apresenta o fluxo de processamento da simulação da plataforma, utilizado para o planejamento de uma QCI. Esse fluxo organiza as etapas desde a modelagem da topologia até a apresentação dos resultados ao usuário, integrando conceitos de teoria de grafos, planejamento de redes ópticas e dimensionamento de recursos quânticos.

O simulador segue um fluxo estruturado em etapas. Inicialmente, a rede é modelada como um grafo $G = (V, E)$, onde os nós representam *data centers* ou pontos de Infraestrutura, e as arestas representam os enlaces ópticos. Em seguida, são definidos os parâmetros de simulação, como a distância máxima suportada por enlace D para um dado SKR e a demanda de chave segura r_k , estabelecendo as restrições físicas e operacionais da rede.

Na sequência, o usuário seleciona a heurística de roteamento (SPSR-Q ou BLQA-Q), que define os caminhos entre os pares de nós. Como os sistemas QKD possuem alcance limitado sem regeneração, a rota é segmentada em trechos que não ultrapassem a distância D , e nos pontos de segmentação são posicionados nós confiáveis (TRNs), cuja quantidade é calculada pela Equação 1.

$$N^k = \left\lceil \sum_{(i,j) \in E} (dist_{ij} x_{ij}^k / D) \right\rceil \lceil (r^k / SKR) \rceil, \quad \forall k \in K \quad (1)$$

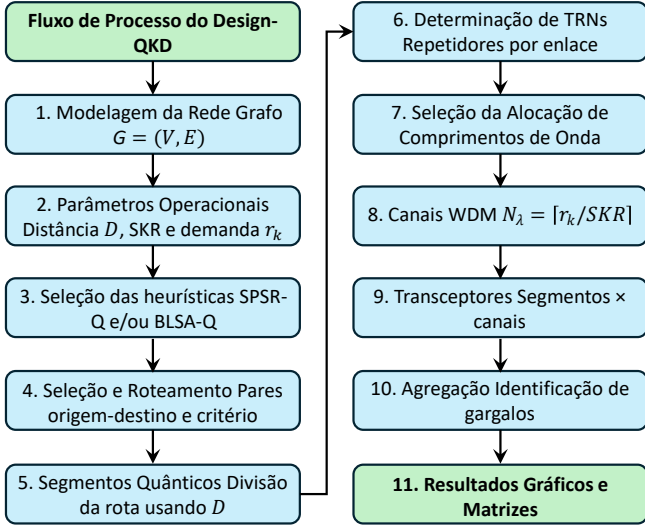


Fig. 1. Fluxo de processo do Design-QKD organizado em duas colunas.

Onde, k representa a requisição, $dist_{ij}$ representa a distância do enlace i e j , x_{ij}^k indica se esse enlace pertence à rota da requisição, D é a distância máxima suportada entre nós quânticos, r^k corresponde à demanda de chave secreta, SKR é a taxa de geração de chaves e K representa o conjunto de requisições.

Definida a rota, escolhe-se o esquema de alocação de recursos (com ou sem conversão de comprimento de onda) e realiza-se o dimensionamento WDM, calculando o número de canais quânticos paralelos necessários por enlace ($N_\lambda = \lceil r_k / SKR \rceil$). A partir desses dados, estima-se o total de transceptores quânticos requeridos, considerando enlaces, canais WDM e TRNs.

Quando há múltiplas demandas simultâneas, a plataforma agrega os recursos calculados individualmente, permitindo avaliar o compartilhamento de enlaces, canais e equipamentos. Por fim, os resultados são consolidados em visualizações gráficas e matrizes, mostrando utilização dos enlaces, distribuição dos TRNs, canais WDM necessários e total de transceptores instalados, fornecendo ao usuário uma avaliação completa do desempenho e dimensionamento da rede projetada.

A. Arquitetura e Framework da Plataforma Computacional

A plataforma adota uma arquitetura cliente-servidor para execução das heurísticas e gerenciamento modular dos componentes. O *frontend* foi desenvolvido em React, permitindo visualização interativa de topologias, configuração dinâmica dos elementos do grafo e geração de gráficos de alocação de recursos. A interface é responsiva e multilíngue (português/inglês). No *backend*, utilizou-se FastAPI e NetworkX para modelagem da rede e execução dos algoritmos de roteamento e busca. A comunicação entre as camadas ocorre por requisições assíncronas em JSON, possibilitando a renderização em tempo real dos resultados da simulação, como TRNs e transceptores.

B. Interface do Usuário

A tela principal é organizada em painéis bem definidos, estruturados para proporcionar clareza operacional e fluidez

na utilização da plataforma. A Figura 2 ilustra a interface principal.

O painel esquerdo reúne as funcionalidades de gerenciamento e edição do projeto. Nesse espaço, o usuário pode abrir e salvar projetos, adicionar nós, criar conexões, remover elementos e limpar completamente a topologia construída. Além disso, o sistema oferece um seletor de topologias pré-definidas, possibilitando o carregamento rápido de dez topologias de exemplo, o que facilita a realização de testes e simulações. A Figura 3 apresenta as seis topologias disponíveis no simulador.

O painel central agrega os principais parâmetros de configuração da simulação. Nesse componente, o usuário especifica a distância máxima D , em quilômetros, entre dois TRNs, definindo, assim, o comprimento máximo de um segmento sem repetidor associado a um determinado valor de SKR . Adicionalmente, é configurada a demanda de taxa de geração de chaves entre o nó de origem s e o nó de destino d , em kbps.

O painel direito reúne as funcionalidades de conversão de comprimentos de onda, seleção de heurísticas e análise de caminhos múltiplos. A organização em painéis segmentados proporciona uma interface intuitiva, estruturada e voltada à configuração precisa dos experimentos.

C. Definição das variáveis para simulação

Como mencionado anteriormente, os parâmetros de distância máxima D , SKR e demanda de taxa de chave podem ser configurados de forma uniforme para toda a topologia ou individualmente por enlace. Essas opções estão disponíveis no painel central da interface (Figura 2).

Ao selecionar a opção de configuração distinta por enlace, o sistema exibe matrizes editáveis para definição individual dos valores de distância, SKR e demanda entre os pares de nós conectados, permitindo representar cenários heterogêneos mais próximos de ambientes reais. Após a configuração dos parâmetros, o usuário pode iniciar a simulação, enviando as matrizes ao *backend* para processamento da alocação de recursos da rede.

D. Heurísticas

As heurísticas são empregadas para resolver problemas de elevada complexidade computacional em tempo viável. Neste trabalho, foram adaptadas de [15] duas heurísticas para o problema de roteamento e alocação de recursos quânticos sobre Infraestruturas ópticas WDM. A SPSR-Q (*Shortest Path with Maximum Spectrum Reuse-Quantum*) realiza o roteamento com base na ordenação crescente das demandas de tráfego e na alocação do primeiro caminho quântico disponível, com ou sem conversão de comprimentos de onda, seguindo abordagem similar ao *First-Fit*. Já a BLSA-Q (*Balanced Load Spectrum Allocation-Quantum*) utiliza balanceamento de carga para minimizar o número máximo de canais quânticos utilizados em cada fibra óptica.

IV. SIMULAÇÕES E RESULTADOS

Após a execução do cálculo, a plataforma apresenta automaticamente os resultados por meio de visualizações gráficas

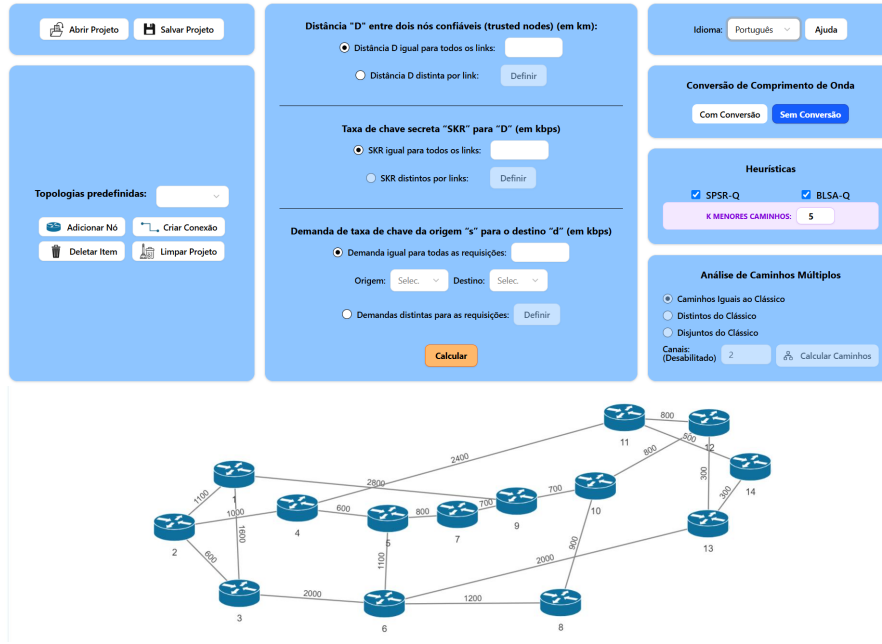


Fig. 2. Interface principal do Design-QKD, com suporte.

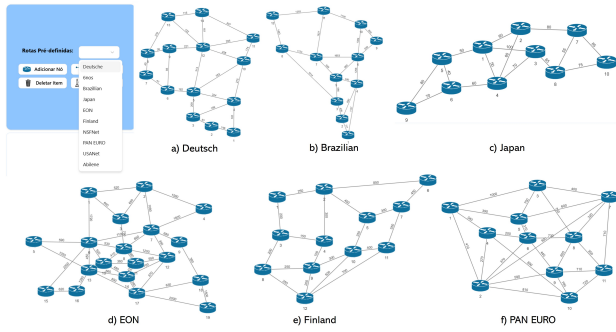


Fig. 3. Seis das dez topologias disponíveis no simulador.

e matrizes de dados, permitindo uma análise estruturada do comportamento da rede e da utilização dos recursos de Infraestrutura.

Como exemplo de aplicação, foi realizada uma simulação utilizando a topologia da rede Pan Euro apresentada na Figura 3f. Nesse cenário, foi considerada uma distância máxima $D = 100$ km entre dois TRNs para um SKR de 50 kbps. As demandas de taxa de chave foram geradas aleatoriamente no intervalo entre 50 kbps e 100 kbps, representando diferentes requisitos de comunicação entre pares de nós da rede. Além disso, a opção de conversão de comprimentos de onda foi selecionada e as duas heurísticas, SPSR-Q e BLSA-Q ($k = 5$).

A partir desses parâmetros, a plataforma gera inicialmente quatro gráficos que sintetizam os principais indicadores operacionais da rede (Figura 4). A Figura 4a apresenta a quantidade de canais WDM utilizados em cada enlace da rede. Esse indicador reflete diretamente a relação entre a demanda de chave segura e o SKR disponível por canal, permitindo identificar enlaces que concentram maior utilização espectral. Em cenários com múltiplas demandas roteadas por caminhos sobrepostos, determinados enlaces passam a atuar como pontos de agregação de tráfego quântico, resultando em maior

consumo de comprimentos de onda.

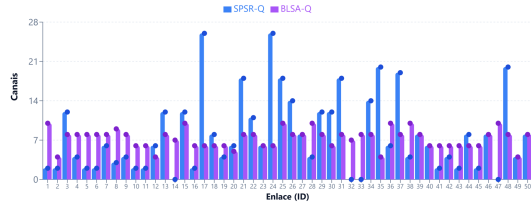
A Figura 4b apresenta a quantidade de transceptores quânticos por enlace, diretamente relacionada ao número de canais WDM alocados. Assim, enlaces com maior concentração de tráfego demandam maior quantidade de *hardware*, impactando o custo da Infraestrutura.

A Figura 4c gráfico apresenta o número de TRNs necessários em cada enlace. Esse indicador está associado principalmente às restrições físicas de transmissão da tecnologia QKD. Como a distância máxima entre dois nós confiáveis é limitada pelo parâmetro D , enlaces mais longos ou caminhos que atravessam regiões extensas da topologia exigem a inserção de múltiplos TRNs para garantir a viabilidade da comunicação quântica.

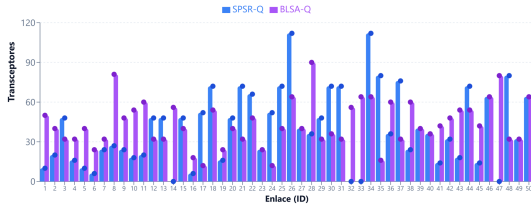
A Figura 4d apresenta um indicador agregado correspondente ao número total de TRNs requeridos para toda a rede. Essa métrica fornece uma visão global da Infraestrutura necessária para suportar o conjunto de demandas consideradas na simulação e permite avaliar o impacto do posicionamento dos repetidores no custo geral da rede. Além das visualizações gráficas, a plataforma também disponibiliza duas matrizes de resultados em formato tabular para cada heurística.

Por fim, observa-se que a heurística SPSR-Q apresenta maior quantidade de canais WDM alocados por priorizar os caminhos mais curtos. Em contrapartida, a BLSA-Q promove melhor balanceamento da utilização dos comprimentos de onda na rede, reduzindo a concentração de canais nos enlaces. Entretanto, por selecionar rotas mais longas e menos congestionadas, essa heurística demanda maior quantidade de TRNs.

Para validar o comportamento do simulador, os resultados obtidos foram comparados com aqueles reportados em [10], que utiliza um modelo baseado em ILP para planejamento de redes QKD.



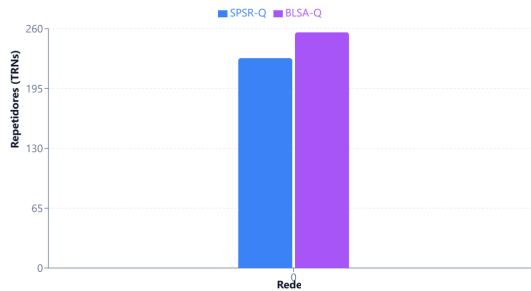
(a) Quantidade de canais WDM alocados por enlace.



(b) Quantidade de transceptores por enlace.



(c) Quantidade de repetidores (TRNs) por enlace.



(d) Quantidade de repetidores (TRNs) na rede.

Fig. 4. Exemplo de gráficos gerados pela plataforma de simulação.

V. CONCLUSÃO

Este trabalho apresentou o desenvolvimento de uma plataforma web voltada ao planejamento de Infraestruturas de comunicação quântica. A ferramenta permite estudar redes de diferentes escalas, desde pequenas topologias até cenários com dezenas de nós, mantendo baixo tempo de resposta nas simulações. A plataforma integra edição de topologias, configuração de parâmetros por matrizes, cálculo de rotas, alocação de recursos e visualização de resultados, possibilitando análise estruturada dos requisitos de Infraestrutura em redes QKD. Como trabalhos futuros, pretende-se expandir a plataforma com novas heurísticas de roteamento e a implementação de mecanismos de análise de resiliência. Também está prevista a inclusão de módulos de simulação para avaliação de fidelidade quântica e modelagem de efeitos lineares e não lineares em fibras ópticas.

AGRADECIMENTOS

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil

(CAPES) - Código de Financiamento 001. O estudo contou ainda com suporte do Programa Interno de Auxílio Financeiro aos Programas de Pós-Graduação Stricto Sensu (AUXPPG) da UEFS e/ou o apoio do Programa de Apoio à Pós-Graduação (PROAP) da CAPES. Por fim, agradecemos ao Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) pelo apoio.

REFERÊNCIAS

- [1] A. K. Fedorov et al. Quantum computing at the quantum advantage threshold: a down-to-business review. *arXiv preprint arXiv:2203.17181*, 2022.
- [2] Sergio Boixo et al. Evidence for quantum annealing with more than one hundred qubits. *Nature Physics*, 10(3):218–224, 2014.
- [3] Google Quantum AI and Collaborators. Quantum error correction below the surface code threshold. *Nature*, 638:920–926, 2025.
- [4] D. Abreu, C. E. Rothenberg, and A. Abelém. Qml-ids: Quantum machine learning intrusion detection system. In *2024 IEEE Symposium on Computers and Communications (ISCC)*, pages 1–6. IEEE, 2024.
- [5] W. Kong, Y. Sun, Y. Gao, and Y.-F. Ji. Coexistence of quantum key distribution and optical communication with amplifiers over multicore fiber. *Nanophotonics*, 12:1979–1994, 2023.
- [6] K. A. Patel et al. Coexistence of high-bit-rate quantum key distribution and data on optical fiber. *Physical Review X*, 2:041010, November 2012.
- [7] I. Maity, J. ur Rehman, and S. Chatzinotas. Taq-net: Traffic-aware minimum-cost quantum communication network planning. *IEEE Transactions on Quantum Engineering*, 6:1–16, 2024.
- [8] R. Ramaswami. *Optical networks: a practical perspective*. Morgan Kaufmann, 2009.
- [9] Y. Cao et al. Cost-efficient quantum key distribution (qkd) over wdm networks. *Journal of Optical Communications and Networking*, 11(6):285–298, 2019.
- [10] F. G. S. Ribeiro, K. D. R. Assis, and R. C. Almeida Jr. Key rate partitioning for enhanced security in qkd-over- wdm networks. *Workshop-Escola de Computação e Informação Quântica e Workshop de Computação Quântica - UFSC. Anais, Florianópolis(SC) UFSC*, 2025.
- [11] Tim Coopmans et al. Netsquid, a network simulator for quantum information using discrete events. *Communications Physics*, 4(1):164, 2021.
- [12] X. Wu et al. Sequence: a customizable discrete-event simulator of quantum networks. *Quantum Science and Technology*, 6(4):045001, 2021.
- [13] S. Diadamo et al. Qunetsim: A software framework for quantum networks. *IEEE Transactions on Quantum Engineering*, 2:1–12, 2021.
- [14] M. Mehic et al. Qkdnetnsim: A simulation framework for quantum key distribution networks. *arXiv preprint arXiv:2005.00017*, 2020.
- [15] Y. Wang et al. A study of the routing and spectrum allocation in spectrum-sliced elastic optical path networks. In *Proc. IEEE INFOCOM*, pages 1503–1511, 2011.