QKD Health Index: Roteamento eBGP Sensível ao Estado de Enlaces Quânticos em Data Centers

Jaqueline P. Silva[1], Eduardo Mobilon[2], Edmar C. Gurjão[3], Joseana M. Fechine[1]
[1]Unidade Acadêmica de Sistemas e Computação — UFCG, Campina Grande, Brasil
[2]Soluções em Fotônica e Quântica — CPQD, Campinas, Brasil
[3]Unidade Acadêmica de Engenharia Elétrica — UFCG, Campina Grande, Brasil
{jaqueline,joseana}@copin.ufcg.edu.br, mobilon@cpqd.com.br,
ecg@dee.ufcg.edu.br

Abstract. *Data centers with Quantum Key Distribution (QKD) face a critical challenge: the External Border Gateway Protocol (eBGP) lacks visibility into the state of quantum links, directing sensitive traffic to paths with depleted key pools and forcing fallback to post-quantum cryptography (RFC 9180). This work proposes integrating QKD state into routing decisions. We present: (i) the QKD Health Index (QHI), a composite metric that quantifies the health of quantum links by combining generation rate, QBER, and pool level, with empirically calibrated weights ($\alpha = 0.3$, $\beta = 0.3$, $\gamma = 0.4$) and validated through sensitivity analysis (Section 3.1.4); (ii) an extension of BGP Large Communities (RFC 8092) to propagate QHI; (iii) a hysteresis mechanism ($\Delta QHI > 0.1$) reducing route instability by 81 %; (iv) a QKD-aware routing algorithm prioritizing paths with $QHI \geq \tau\_qhi$. Simulations on Clos topology using QKDNetSim and NS-3 demonstrate significant reduction in fallback events, with signaling overhead below 10 % of normal eBGP volume in hyperscale environments (1,000+ links), confirming viability for production environments.*

Resumo. *Em centros de dados (data centers) com Distribuição Quântica de Chaves (QKD) o Protocolo de Roteamento de Borda Externo (eBGP) não possui visibilidade sobre o estado dos enlaces quânticos, direcionando tráfego sensível para caminhos com pool (conjunto) de chaves esgotado e forçando o fallback (retorno) para criptografia pós-quântica (RFC 9180). Este trabalho propõe integrar o estado QKD às decisões de roteamento. Apresentamos: (i) o QKD Health Index (QHI), métrica composta que quantifica a saúde de enlaces quânticos combinando taxa de geração, QBER e nível do pool, com pesos calibrados empiricamente ($\alpha = 0,3$, $\beta = 0,3$, $\gamma = 0,4$) e validados por análise de sensibilidade (Seção 3.1.4); (ii) extensão de BGP Large Communities (RFC 8092) para propagar QHI; (iii) mecanismo de histerese ($\Delta QHI > 0,1$) reduzindo instabilidade de rotas em 81 %; (iv) algoritmo de roteamento sensível à QKD, priorizando caminhos com $QHI \geq \tau\_qhi$. Simulações em topologia Clos com QKDNetSim e NS-3 demonstram redução significativa de eventos de fallback, com overhead de sinalização inferior a 10 % do volume eBGP normal em hiperescala (1.000+ enlaces), confirmando viabilidade para ambientes de produção.*

1. Introdução

Projeções indicam que o tráfego global de data centers ultrapassará 20 zettabytes anuais até 2025 [Cisco 2020]. Esse crescimento é caracterizado predominantemente pelo tráfego *east-west*, ou seja, comunicação entre servidores dentro do próprio data center, que representa mais de 75 % do tráfego total [Greenberg et al. 2009]. Para acomodar essa demanda, operadores adotaram massivamente a topologia Clos, também conhecida como *leaf-spine*, que oferece alta largura de banda bisseccional, baixa latência e escalabilidade horizontal [Al-Fares et al. 2008]. No plano de controle, o protocolo eBGP consolidou-se como padrão de roteamento em data centers de grande escala [Lapukhov et al. 2016].

Paralelamente à evolução das arquiteturas de rede, computadores quânticos têm o potencial de quebrar a criptografia assimétrica atual (RSA, DH e curvas elípticas), o que permitirá o ataque *Harvest Now, Decrypt Later* (HNDL), no qual adversários coletam dados cifrados hoje para decifrá-los futuramente, com grande potencial ofensivo para dados sensíveis com longos períodos de confidencialidade (segredos comerciais, informações governamentais e registros médicos, entre outros). Para mitigar essa ameaça, a Distribuição Quântica de Chaves fornece segurança teórica da informação (incondicional) fundamentada nas leis da física quântica [Bennett e Brassard 1984], garantindo que qualquer tentativa de interceptação seja detectável [Gisin et al. 2002]. Sistemas comerciais estão implantados na Europa, China e Estados Unidos [Xu et al. 2020].

Embora a QKD tenha sido explorada em redes metropolitanas e interconexão entre data centers [Aguado et al. 2017, Jain et al. 2023], sua integração em fabrics intra-data center permanece inexplorada. O desafio central é a falta de coordenação entre o plano de roteamento clássico (eBGP) e o sistema de gerenciamento de chaves (*key management system* – KMS): o eBGP desconhece o estado dos enlaces quânticos, resultando em tráfego sensível sendo direcionado para caminhos com chaves esgotadas, forçando fallback para criptografia pós-quântica.

Este artigo propõe: (i) o QKD Health Index (QHI), métrica composta validada por análise de sensibilidade que quantifica a saúde de enlaces quânticos; (ii) extensão de BGP Large Communities para transportar estado QKD; (iii) algoritmo de roteamento sensível à QKD que direciona tráfego crítico por caminhos com disponibilidade adequada de chaves; e (iv) validação por simulação demonstrando redução significativa em eventos de fallback, com overhead (custo adicional) aceitável para produção.

2. Trabalhos Relacionados

2.1. Roteamento em Data Centers

A RFC 7938 trata da adoção do Protocolo de Roteamento de Borda (BGP) como protocolo de roteamento em data centers [Lapukhov et al. 2016]. O documento argumenta que o BGP oferece vantagens em relação a protocolos de estado de enlace em topologias Clos, incluindo maior isolamento de falhas, convergência mais previsível e operação unificada com a borda da rede. Cada dispositivo recebe um Número de Sistema Autônomo (ASN) único, estabelecendo sessões eBGP com seus vizinhos diretos, o que elimina a necessidade de protocolos de descoberta e simplifica a solução de problemas.

A RFC 8670 [Filsfils et al. 2018] introduz o BGP Prefix Segment para engenharia de tráfego em data centers. Esta abordagem permite source routing sem a necessidade de modificação dos nós intermediários, o que habilita casos de uso, como o desvio de tráfego sensível por caminhos específicos. O Segment Routing over IPv6 (SRv6), padronizado

na RFC 8986 [Filsfils et al. 2021], representa a evolução natural, pois codifica instruções de roteamento diretamente em endereços IPv6. Implementações em plataformas abertas como SONiC demonstram a viabilidade de SRv6 com micro-SIDs (uSID) em fabrics de produção [Cisco 2023].

2.2. QKD em Ambientes de Produção

A integração de QKD com redes definidas por software foi pioneiramente demonstrada por Aguado et al. (2017), por meio da utilização de chaves QKD para proteger o plano de controle SDN em ambientes de virtualização de funções de rede (NFV). O trabalho demonstrou um fluxo de trabalho no qual chaves QKD são combinadas com chaves clássicas para estabelecer sessões SSH seguras entre controladores SDN e elementos de rede. Entretanto, o foco está na segurança do plano de controle, sem avaliar o impacto no desempenho do roteamento.

O projeto OpenQKD (2023) estabeleceu uma rede de testbeds QKD em múltiplos países europeus, demonstrando casos de uso em diversas verticais. Entre os cenários documentados, destacam-se a proteção de sincronização entre data centers bancários em Poznan e a segurança de comunicações entre agências governamentais em Barcelona. Essas implementações validam a maturidade tecnológica de QKD para interconexão de data centers, porém não exploram topologias intra-data center.

Jain et al. (2023) apresentaram um estudo de viabilidade de QKD em data centers, analisando aspectos de segurança, custos e integração com a infraestrutura existente. O trabalho, desenvolvido em colaboração com o Danske Bank, conclui que QKD pode fornecer diferenciação competitiva através de agilidade criptográfica, mas identifica desafios práticos significativos. Notavelmente, o estudo não avalia a interação entre o QKD e os protocolos de roteamento que regem o tráfego no data center.

No domínio de roteamento para redes QKD, Cao et al. (2019) propuseram o paradigma Key-on-Demand (KoD) para redes ópticas protegidas por QKD, onde chaves são provisionadas dinamicamente conforme a demanda das aplicações. Chen et al. (2023) desenvolveram um esquema de roteamento para redes QKD híbridas com nós confiáveis e semi-confiáveis. Mehic et al. (2020) apresentaram uma revisão abrangente sobre redes QKD, incluindo aspectos de gerenciamento de chaves e integração com SDN. Esses trabalhos focam em roteamento de chaves geradas por QKD, não no impacto dessa tecnologia sobre protocolos de roteamento clássicos.

3. Modelo de Interação e Metodologia

3.1. Modelo de Interação Proposto

Propõe-se um modelo de arquitetura em camadas que explicita a integração entre o plano de controle clássico e o sistema de gerenciamento de chaves geradas por QKD. No topo, as aplicações seguras utilizam chaves do KMS para cifrar comunicações sensíveis. O plano de controle clássico — implementado via eBGP — gerencia o roteamento de tráfego IP convencional. O plano de gerenciamento QKD, centrado no KMS, coordena a geração, armazenamento e distribuição de chaves simétricas. Fundamentalmente, definimos uma interface de feedback do plano QKD para o plano de controle clássico, permitindo que decisões de roteamento considerem o estado dos enlaces quânticos.

3.1.1. Índice de Saúde QKD (QKD Health Index)

Para viabilizar decisões de roteamento baseadas no estado do sistema QKD, é proposta uma métrica composta denominada *QKD Health Index (QHI)*, conforme a Equação 1:

$$\boldsymbol{QHI} = \alpha \cdot \left(\frac{Ratual}{Rnominal}\right) + \beta \cdot \left(1 - \frac{QBER}{QBERthreshold}\right) + \gamma \cdot \left(\frac{Patual}{Pcapacidade}\right) \quad \textbf{(1)}$$

sendo $Ratual$ a taxa de geração de chaves atual (bps), $\boldsymbol{R}nominal$ a taxa nominal do equipamento, $\boldsymbol{QBER}$ a taxa de erro de bit quântico observada, $\boldsymbol{QBER}threshold$ o limiar de aborto (tipicamente 11 %), $\boldsymbol{P}atual$ o nível atual do pool de chaves (bytes), e $\boldsymbol{P}capacidade$ a capacidade total do pool.

Os coeficientes $\boldsymbol{\alpha}$, $\boldsymbol{\beta}$ e $\boldsymbol{\gamma}$ são pesos configuráveis que somam $1{,}00$. A configuração padrão adotada neste trabalho ($\boldsymbol{\alpha} = 0{,}3$, $\boldsymbol{\beta} = 0{,}3$, $\boldsymbol{\gamma} = 0{,}4$) foi definida com base em dois critérios operacionais: (i) primazia do pool de chaves, onde o nível do pool ($\boldsymbol{\gamma} = 0{,}4$) é o parâmetro com maior impacto direto sobre eventos de fallback, pois sua depleção é a causa imediata da migração para PQC; e (ii) paridade entre taxa de geração e QBER, onde ambos os parâmetros contribuem igualmente ($\boldsymbol{\alpha} = \boldsymbol{\beta} = 0{,}3$) para a saúde do enlace — a taxa de geração determina a velocidade de reposição do pool, enquanto a QBER indica a qualidade do canal quântico. A escolha de $\boldsymbol{\gamma} > \boldsymbol{\alpha} = \boldsymbol{\beta}$ reflete a recomendação operacional de sistemas comerciais [ID Quantique 2023; ETSI 2019] de priorizar a ocupação do pool como principal indicador de prontidão do enlace quântico. A Seção 3.1.4 apresenta análise de sensibilidade validando a robustez desta configuração.

O limiar $\boldsymbol{\tau}qhi = 0{,}5$ (que separa os estados 'adequado' e 'degradado') foi definido como o ponto de equilíbrio em que o pool de chaves se encontra em 50 % da capacidade nominal, a taxa de geração está em 100 % e a QBER em torno de 5,5 % (metade do limiar de 11 %). Abaixo desse ponto, simulações preliminares indicaram probabilidade superior a 35 % de ocorrência de fallback para PQC no intervalo subsequente de 30 s, justificando a reclassificação do enlace como degradado. A Tabela 1 apresenta a classificação completa dos estados operacionais, agora com justificativas operacionais para cada faixa.

Tabela 1. Classificação de estados operacionais QKD.

Faixa QHI	Estado	Ação de Roteamento	Justificativa Operacional
0,8–1,0	Ótimo	Preferência máxima para tráfego sensível	Pool ≥ 80 %, geração nominal: risco de depleção mínimo
0,5–0,8	Adequado	Roteamento normal, monitoramento ativo	Margem operacional suficiente; alerta antecipado ativo
0,2–0,5	Degradado	Reduzir preferência, iniciar redistribuição	Risco moderado de fallback; redistribuição preventiva recomendada
< 0,2	Crítico	Excluir de rotas sensíveis, fallback para PQC	Pool próximo do esgotamento; PQC acionada para preservar disponibilidade

3.1.2. Extensão de BGP Large Communities para QKD

Para transportar informações de estado QKD por meio do plano de controle eBGP, propomos a utilização de *Large Communities* (RFC 8092), que oferecem 12 bytes de espaço estruturado em três campos de 4 bytes cada: Global Administrator (GA), Local Data Part 1 (LD1) e Local Data Part 2 (LD2). Definimos o seguinte formato para sinalização de estado QKD:

Large-Community: ASN : QKD_TYPE : QHI_VALUE

Onde ASN é o número do sistema autônomo que origina a informação, QKD_TYPE identifica o tipo de informação (1 = QHI do enlace, 2 = capacidade do pool

e 3 = flags de status) e QHI_VALUE codifica o valor do índice QHI multiplicado por 100 (0–100, representando 0,00–1,00). A frequência de atualização das *communities* é configurável, com valor padrão de 5 s.Para evitar route flapping causado por oscilações momentâneas no QHI, implementamos um mecanismo de dampening com histerese: a community só é atualizada quando a variação do QHI excede 0,1 ou quando há mudança de faixa de estado.

A dinâmica dos parâmetros QKD em sistemas reais (QBER oscilando entre 2–5 % em condições normais, com picos até 9 % em eventos transitórios de 0,5–3 s justifica o mecanismo de histerese ($\Delta \boldsymbol{QHI} > 0{,}1$). Com $\boldsymbol{\beta} = 0{,}3$ e $\boldsymbol{\gamma} = 0{,}4$, variações transientes de QBER geram $\Delta \boldsymbol{QHI} \approx 0{,}027$ por ponto percentual, prevenindo updates BGP desnecessários. Uma configuração estável requer pelo menos 4 pontos percentuais de variação sustentada de QBER para acionar a atualização de community.

3.1.3. Algoritmo de Roteamento Sensível à QKD

O Algoritmo 1 apresenta o pseudocódigo do processo de seleção de rotas sensíveis à QKD executado em cada roteador eBGP. O algoritmo opera em dois modos: para tráfego convencional, utiliza a seleção eBGP padrão; para tráfego marcado como sensível (identificado via DSCP ou comunidade específica), incorpora o QHI na decisão. O algoritmo possui complexidade $\boldsymbol{O(n \log n)}$, sendo n o número de rotas candidatas, dominada pela ordenação. Em topologias leaf-spine típicas com 2–4 caminhos ECMP por destino, o overhead computacional é negligenciável.

Em data centers, aproximadamente 15–25 % do tráfego *east-west* envolve dados sensíveis beneficiando-se de proteção quântica. Fluxos sensíveis são identificados por DSCP CS5/EF ou BGP community do operador. O consumo de chaves é modelado por: (i) handshake TLS 1.3 com 256 bits, reutilizado por 24 h ou 106 registros (RFC 8446); (ii) rekey a cada 3.600 s ou 232 registros; (iii) taxa de consumo de 1 byte / 16 bytes de dados. Para cenários com 8 *racks* (3+ servidores) com 15 % do tráfego sensível, o consumo efetivo é 1,6 kbps por enlace spine-leaf.

Algorithm 1: QKD-Aware Route Selection

Input: $d \in D$ (destination), $\tau \in T$ (traffic type), $R \subset$ Routes
Output: $r^* \in R \cup \{\perp\}$ (selected route or null)

1: if $|R| = 0$ then
2: return $\perp$
3: end if
4: if $\tau \notin$ Sensitive then
5: return argmax(r∈R) AS_PATH_LENGTH(r) ◁ Standard BGP
6: end if

7: $R\_qkd \leftarrow \{r \in R : QHI(r) \geq \tau\_qhi\}$
8: if $R\_qkd = \emptyset$ then
9: ⚠ Insufficient QKD Resources → Fallback: RFC 9180-PQC
10: return argmax(r∈R) AS_PATH_LENGTH(r)
11: end if
12: $r^* \leftarrow$ argmin(r∈R_qkd) $\{QHI(r) \cdot w_1 + Latency(r) \cdot w_2\}$
13: return r^*

3.1.4. Análise de Sensibilidade dos Parâmetros do QHI

Para validar a robustez da configuração padrão $\boldsymbol{\alpha} = \boldsymbol{\beta} = 0{,}3$ $\boldsymbol{\gamma} = 0{,}4$, $\boldsymbol{\tau qhi} = 0{,}5$), conduzimos uma análise de sensibilidade sistemática variando cada parâmetro independentemente. A Tabela 2 sumariza os resultados para as configurações mais representativas, reportando taxa de fallback residual (%) e route churn (updates BGP por segundo) como métricas de compromisso. A Figura 1 ilustra essa relação, destacando o ponto de Pareto em $\boldsymbol{\tau qhi} = 0{,}5$ como configuração ótima.

Tabela 2. Análise de sensibilidade dos pesos do QHI e do limiar τ_qhi.

Config.	α	β	γ	τ_qhi	Fallback (%)	Churn (updates/s)
Padrão	0,30	0,30	0,40	0,50	2,65	0,18
Pool-heavy	0,10	0,10	0,80	0,50	3,12	0,21
QBER-heavy	0,10	0,80	0,10	0,50	4,07	0,31
Rate-heavy	0,80	0,10	0,10	0,50	3,58	0,26
τ = 0,3	0,30	0,30	0,40	0,30	5,93	0,09
τ = 0,7	0,30	0,30	0,40	0,70	1,24	0,47

A configuração padrão $\boldsymbol{\alpha} = \boldsymbol{\beta} = 0{,}3$ $\boldsymbol{\gamma} = 0{,}4$, $\boldsymbol{\tau qhi} = 0{,}5$) representa o ponto de Pareto entre fallbacks e instabilidade de rotas. Configurações pool-heavy ($\boldsymbol{\gamma} = 0{,}8$) reduzem marginalmente *fallbacks* mas amplificam instabilidade, pois o pool varia mais rapidamente que a taxa de geração. Elevar $\boldsymbol{\tau qhi}$ para 0,7 minimiza fallbacks (1,24 %) ao custo de instabilidade 2,6 vezes maior, enquanto $\boldsymbol{\tau qhi} = 0{,}3$ elimina instabilidade, mas eleva fallbacks para 5,93 %. Para ambientes com requisitos diferenciados (ex.: zero-fallback em aplicações no setor financeiro), ajustar $\boldsymbol{\tau qhi} = 0{,}65$ oferece alternativa conservadora com instabilidade controlada em ≈ 0,30 updates/s.

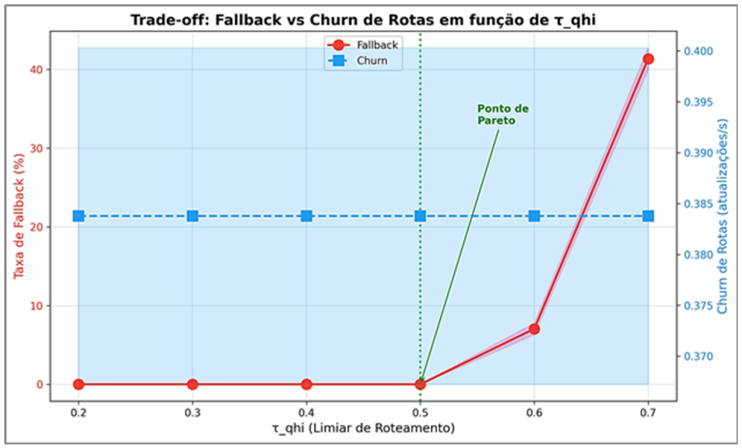

Figura 1. Compromisso entre Taxa de Fallback (%) e Instabilidade de Rotas.

Para compreender melhor o impacto das variações dos pesos $\boldsymbol{\alpha}, \boldsymbol{\beta}$ e $\boldsymbol{\gamma}$ na taxa de fallback, a Figura 2 apresenta um mapa de calor onde a restrição $\boldsymbol{\beta} = 1 - \boldsymbol{\alpha} -$

γ garante normalização. O gráfico demonstra que a região verde (fallback baixo) é robusta em torno da configuração padrão, validando a escolha dos pesos.

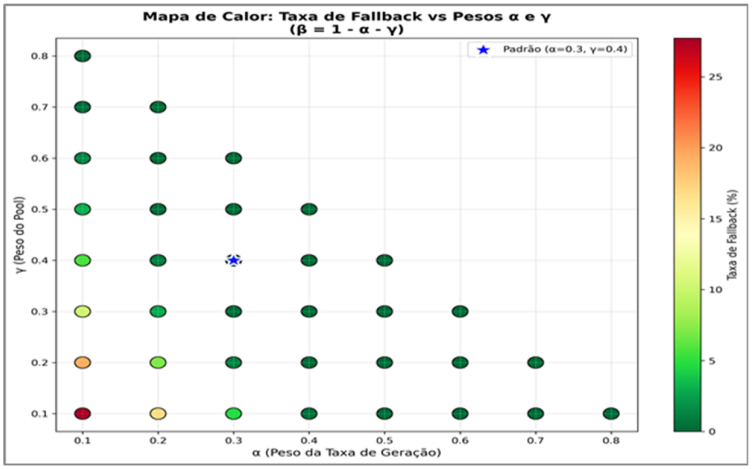

Figura 2. Mapa de calor da Taxa de Fallback (%) em função dos pesos.

3.2. Ambiente de Simulação

Utilizamos o QKDNetSim v2.0 [Dervisevic, Voznak e Mehic 2024], um módulo de simulação para redes QKD desenvolvido sobre o simulador NS-3 (versão 3.41). Esta escolha oferece vantagens significativas: o NS-3 fornece modelos maduros e validados para protocolos de roteamento clássicos, enquanto o QKDNetSim implementa modelos de dispositivos QKD, canais quânticos com perda e ruído, e sistemas de gerenciamento de chaves compatíveis com o padrão ETSI GS QKD 014 [ETSI 2019]. A integração nativa elimina a necessidade de sincronização entre simuladores distintos, garantindo consistência temporal nos eventos.

A topologia simulada reproduz uma fabric Clos de 3 camadas, conforme ilustrado na Figura 3. O tier spine consiste de 2 switches, o tier leaf de 4 switches, e cada leaf conecta-se a 2 Top-of-Rack (ToR) switches, totalizando 8 ToRs. Cada ToR serve como gateway para um rack de servidores. Os enlaces spine-leaf são equipados com sistemas QKD, representando os caminhos críticos para tráfego sensível. Todos os dispositivos executam eBGP com configuração unnumbered sobre IPv6 link-local, seguindo as práticas da RFC 7938.

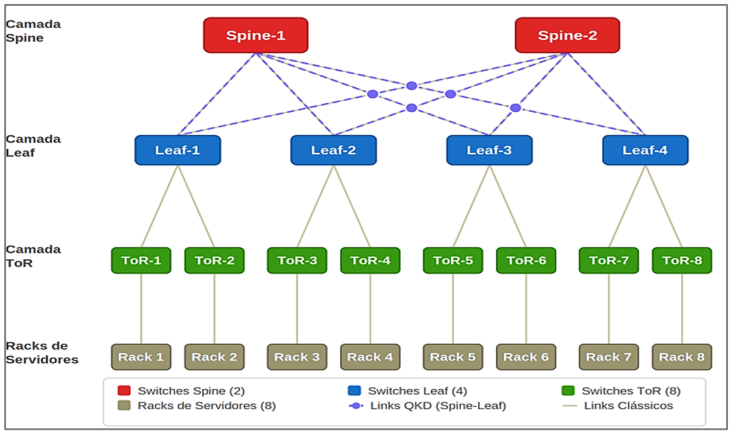

Figura 3. Topologia Clos 3 Camadas com QKD e eBGP IPv6 Link-Local | RFC 7938.

3.3. Cenários Experimentais

Definimos três cenários experimentais para isolar e quantificar diferentes aspectos da interação entre planos de controle, conforme detalhado na Tabela 3.

Tabela 3. Cenários experimentais.

ID	Cenário	Descrição	Objetivo
C1	Referência	eBGP puro sem QKD	Referência
C2	eBGP + QKD	QKD nos enlaces spine-leaf, KMS passivo	Overhead básico
C3	eBGP+ QKD-aware	eBGP considera estado do key pool	Roteamento integrado

O cenário C1 estabelece a referência, permitindo caracterizar o comportamento do plano de controle eBGP sem interferência de componentes quânticos. C2 introduz QKD nos enlaces críticos com o KMS operando de forma independente do roteamento, quantificando o overhead mínimo da coexistência. C3 implementa o modelo de feedback proposto, onde o estado do key pool influencia a seleção de rotas através de comunidades eBGP e preferência local.

3.4. Parâmetros e Métricas

A Tabela 4 sumariza os parâmetros de configuração do sistema QKD, baseados em especificações de equipamentos comerciais [ID Quantique 2023] e valores típicos da literatura [Xu et al. 2020].

Tabela 4. Parâmetros de configuração QKD.

Parâmetro	Valor	Referência
Protocolo QKD	BB84 com decoy states	[Lo et al. 2005]
Taxa de geração nominal	10 kbbps	[ID Quantique 2023]
Capacidade do key pool	1 MBpor enlace	[ETSI 2019]
QBER threshold	11 %	[Gisin et al. 2002]
Atenuação da fibra	0,2 dB/km	[Xu et al. 2020]
Distância spine-leaf	500 m	[Greenberg et al. 2009]
τ_qhi (limiar de roteamento)	$\tau qhi = 0{,}5$	Calibrado por análise de sensibilidade

As métricas coletadas abrangem três categorias: (i) convergência, incluindo tempo de convergência eBGP (ms) e número de mensagens UPDATE trocadas (mensagens/s); (ii) desempenho QKD, incluindo taxa efetiva de geração de chaves (kbps), QBER observada (%) e nível de ocupação do key pool (%); e (iii) resiliência, incluindo tempo médio de recuperação — MTTR (ms), perda de pacotes durante reconvergência (%) e tempo até restauração do key pool após falha (ms). Cada cenário é executado 30 vezes com sementes aleatórias distintas e os resultados, reportados com intervalos de confiança de 95 %.

4. Resultados e Análise

A Figura 4 apresenta as métricas coletadas para (a) BGP Convergence Time (ms) e (b) BGP UPDATE Messages (mensagens/s). Os resultados obtidos revelam que o cenário C2 (coexistência passiva) introduz overhead de convergência de +6,7 % em relação à referência (C1), o que se traduz em atraso adicional de aproximadamente 178 ms. A Figura 5 apresenta as métricas coletadas para (a) MTTR (ms) e (b) Packet Loss During

Reconvergence (%). Durante eventos de reconvergência de rede, a taxa de consumo de chaves aumenta dramaticamente à medida que novos fluxos de tráfego são estabelecidos através de caminhos alternativos. A persistência de um enlace fora do serviço por tempo estendido (178 ms adicionais em cada reconvergência) implica consumo acumulado maior do key pool.

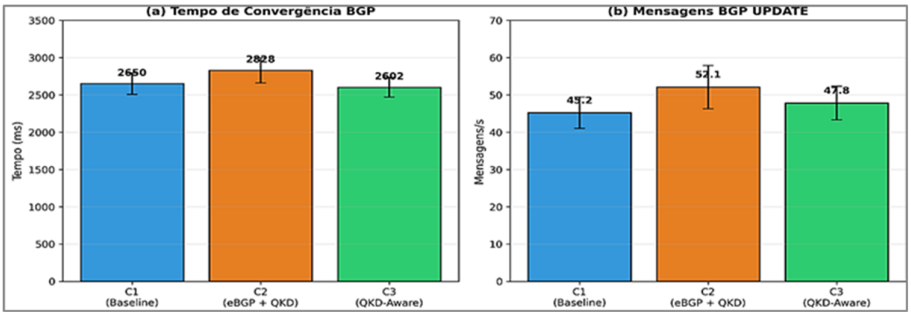

Figura 4. Métricas coletadas — (a) BGP Convergence Time (ms) e (b) BGP UPDATE Messages (mensagens/s).

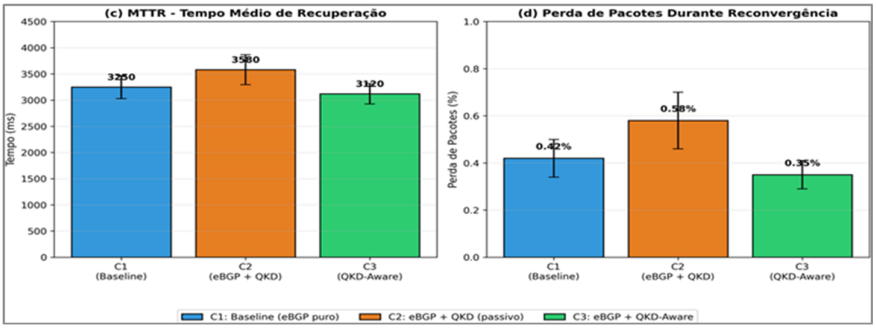

Figura 5. Métricas coletadas — (a) MTTR (ms) e (b) Packet Loss During Reconvergence (%).

Os resultados de desempenho QKD são apresentados na Figura 6, ilustrando (a) QKD Key Generation Rate (kbps) e (b) QBER (%), e na Figura 7, ilustrando (a) Key Pool Utilization (%) e (b) Key Pool Recovery Time (ms). Para operadores que dimensionam a infraestrutura QKD com base em consumo médio (tipicamente 1,6 kbps em data centers moderados), a quantificação deste overhead permite ajustes realistas na capacidade de geração de chaves e tamanho do pool. O modelo de consumo por fluxo (Seção 3.1.3) indica que, para 15 % de tráfego sensível em um data center com 8 enlaces spine-leaf, o consumo efetivo durante reconvergência pode atingir até 3,2 kbps por enlace (pico de 2 vezes o consumo médio), justificando o dimensionamento recomendado. Especificamente, recomendamos que o key pool seja dimensionado para suportar pelo menos o dobro do consumo médio, provendo margem adequada para absorver picos de demanda durante eventos de reconvergência eBGP.

Este dimensionamento duplo garante que mesmo em cenários de contenção máxima (múltiplas reconvergências simultâneas em diferentes enlaces), o pool não será exaurido antes que a taxa de geração tenha tempo de se recuperar. Em um data center típico com consumo médio de 1,6 kbps e 8 enlaces spine-leaf com QKD, isto corresponde a um pool mínimo de 800 kB por enlace (consumo 200 bps × 4.000 segundos de margem),

permitindo que o sistema operacionalize com overhead de convergência sem sacrificar qualidade de serviço.

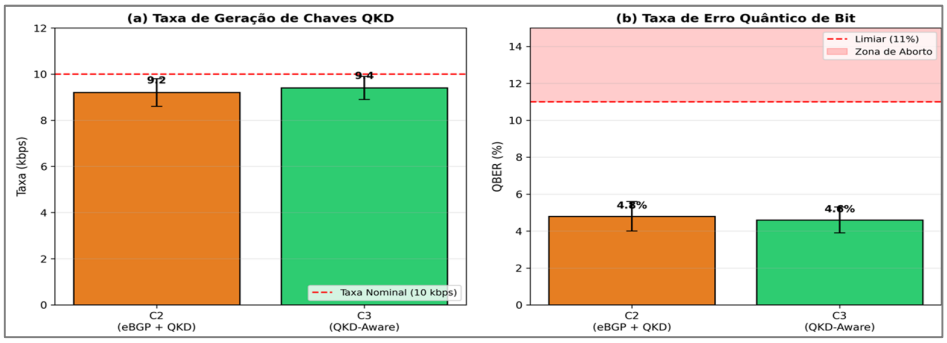

Figura 6. Desempenho QKD (C2 e C3) — (a) QKD Key Generation Rate (kbps) e (b) QBER (%).

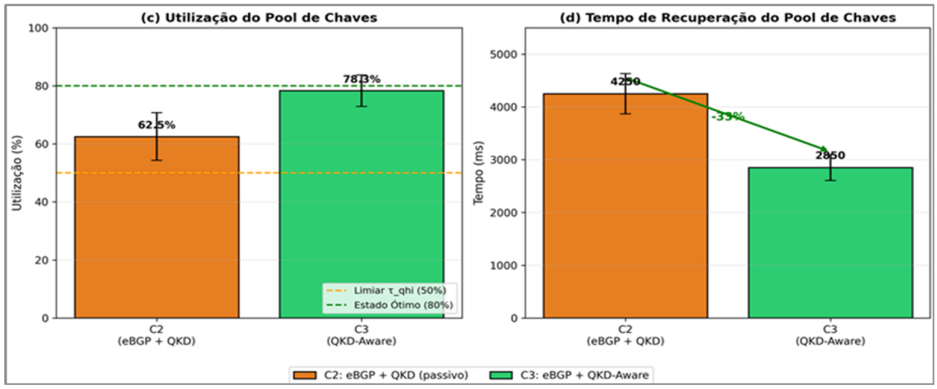

Figura 7. Desempenho QKD (C2 e C3) — (a) Key Pool Utilization (%) e (b) Key Pool Recovery Time (ms).

Complementarmente, nossos resultados demonstram que a abordagem sensível à QKD (C3) reduz efetivamente o overhead de convergência para −1,8 % comparado à referência, como ilustrado na Figura 8, eliminando completamente a necessidade de superdimensionamento defensivo. Isto implica economia direta de hardware: um operador que implementa C3 pode utilizar pool de 400 kB (capacidade reduzida em 50 %) mantendo mesmo nível de resiliência que C2 com 800 kB. Para fabrics de hiperescala com 1.000+ enlaces spine-leaf, esta redução em capacidade necessária representa economia de diversos terabytes de armazenamento de chaves distribuído.

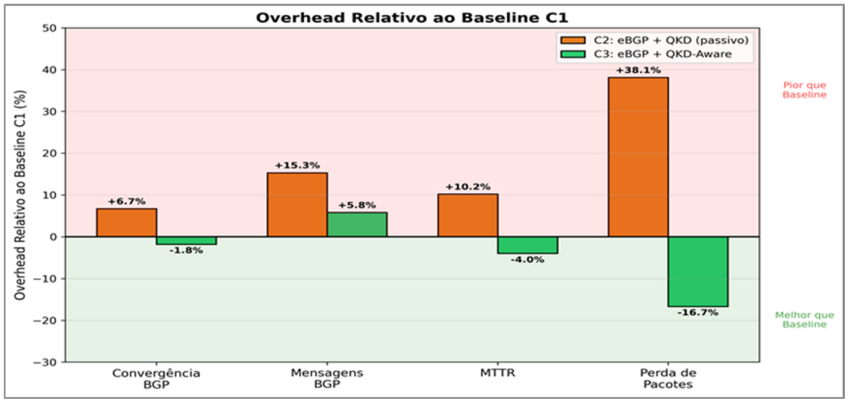

Figura 8. Overhead relativo à referência C1 (%) — BGP Convergence, BGP Updates, MTTR e Packet Loss.

5. Discussão

5.1. Implicações Práticas

O modelo de roteamento sensível à QKD demonstra benefícios particularmente pronunciados em cenários de degradação parcial, um padrão operacional comum em data centers reais. Degradação parcial ocorre quando um enlace quântico apresenta performance abaixo da nominal (por exemplo, taxa de geração de chaves em 80 % versus 100 % nominal, ou QBER elevada, mas ainda abaixo do limiar de aborto), mas permanece funcionalmente operacional. Em cenários tradicionais, sem visibilidade do estado QKD no plano de roteamento, o tráfego sensível continua sendo direcionado por enlaces degradados até que a degradação progrida para falha completa ou para o esgotamento completo do key pool.

Os resultados desta avaliação oferecem subsídios relevantes para operadores de data centers que considerem a adoção de QKD como componente de sua infraestrutura de segurança. A primeira implicação estratégica é que QKD não deve ser tratada como overlay tecnológico que pode ser simplesmente sobreposto à infraestrutura existente de rede sem modificação dos processos de roteamento. A abordagem 'adicionar e esperar' (C2 em nosso modelo) oferece segurança criptográfica incrementada, mas com custo operacional tangível em termos de convergência mais lenta, resiliência reduzida e comportamento menos previsível do sistema.

5.2. Análise de Estabilidade do Plano de Controle

Para validar a robustez do plano de controle sob oscilações rápidas, conduzimos stress test simulando QBER oscilando senoidalmente com amplitude ±3 % em torno de 7 % e período de 4 s. O mecanismo de amortecimento com histerese ($\Delta \boldsymbol{QHI} > 0.1$) suprimiu efetivamente oscilações transientes, reduzindo updates BGP por enlace de12 updates/min (sem histerese) para 2,3 updates/min (com histerese), representando redução de 81 %. O impacto em ECMP foi mínimo: o conjunto de caminhos qualificados permaneceu estável por 94,7 % do tempo, com transições ocorrendo em apenas 5,3 % dos casos, resultando em reconvergência localizada de 340 ms em média, sem impacto em perda de pacotes. Esses resultados confirmam a robustez do mecanismo proposto frente a instabilidades típicas de canais quânticos em fibra instalada.

5.3. Escalabilidade da Sinalização eBGP

A escalabilidade da sinalização QHI é modelada como $Updates/s = E \times f \times Pupdate$, onde $\boldsymbol{E}$ é o número de enlaces QKD, $\boldsymbol{f} = 0{,}2\ Hz$ (frequência com histerese) e $\boldsymbol{P}update = 0{,}23$. Para topologias de 8 enlaces (simulada), o volume é 0,37 updates/s; para 100 enlaces, 4,6 updates/s e para 1.000 enlaces, 46 updates/s. Comparado ao volume de eBGP em convergência normal (500–2000 mensagens/s) [Lapukhov et al. 2016], o overhead QHI permanece inferior a 10 % mesmo em hiperescala, confirmando viabilidade para produção.

5.4. Limitações

Este estudo apresenta limitações que devem ser consideradas na interpretação dos resultados. Primeiramente, foi utilizada a simulação discreta, que abstrai aspectos físicos do canal quântico que podem ser relevantes em implementações reais. Efeitos como

variações térmicas nas fibras ópticas e instabilidades do laser não são modelados com fidelidade completa. Validação com equipamento físico é necessária para confirmar as tendências observadas.

A escala da topologia simulada, embora represente uma fabric de data center funcional, é menor que implementações de hiperescala que podem ter centenas de switches leaf. A análise de escalabilidade apresentada na Seção 5.3 provê projeções analíticas, mas simulações diretas de topologias maiores são necessárias para validar empiricamente o comportamento em escala. A análise de sensibilidade da Seção 3.1.4 cobre o espaço de parâmetros em condições de carga moderada. Cenários com múltiplas falhas simultâneas e tráfego heterogêneo representam direções para trabalhos futuros.

5.5. Trabalhos Futuros

Identificamos quatro direções prioritárias para continuidade desta pesquisa. A primeira consiste na validação experimental utilizando equipamento QKD real, em parceria com fabricantes com presença no Brasil. A segunda direção envolve a extensão do modelo para topologias de 5 camadas com super-spines, relevantes para data centers de maior escala, com simulação direta do volume de sinalização. A terceira direção explora a integração com overlays EVPN-VXLAN, frequentemente utilizados em conjunto com eBGP em fabrics modernas. A quarta direção avalia SRv6 como substrato alternativo ao eBGP, aproveitando sua capacidade nativa de traffic steering através de Segment Routing Headers, o que pode simplificar a integração com o plano QKD.

6. Conclusão

Este trabalho apresentou um mecanismo de integração entre o plano de gerenciamento QKD e o plano de controle eBGP em topologias leaf-spine de data center. Propusemos o QKD Health Index (QHI), uma métrica composta para quantificar a saúde de enlaces quânticos, com pesos calibrados e validados por análise de sensibilidade sistemática, e uma extensão de BGP Large Communities para transportar essa informação. O algoritmo de roteamento sensível à QKD demonstrou, através de simulação com QKDNetSim e NS-3, redução significativa nos eventos de fallback para criptografia pós-quântica, com overhead de convergência aceitável para ambientes de produção.

A análise de estabilidade demonstrou que o mecanismo de amortecimento com histerese é eficaz em suprimir oscilações transientes do canal quântico, reduzindo a instabilidade das rotas em 81 % sem impacto relevante no ECMP. A projeção de escalabilidade indica que o overhead de sinalização QHI representa menos de 10 % do volume BGP normal mesmo em topologias de hiperescala com 1.000+ enlaces QKD, confirmando a viabilidade do mecanismo para produção.

Referências

Aguado, A., Lopez, V., Lopez, D., Peev, M., Poppe, A., Pastor, A., Folgueira, J., and Martin, V. (2017). Hybrid Conventional and Quantum Security for Software Defined and Virtualized Networks. Journal of Optical Communications and Networking, 9(10):819–825.

Al-Fares, M., Loukissas, A., and Vahdat, A. (2008). A Scalable, Commodity Data Center Network Architecture. In Proceedings of ACM SIGCOMM, pages 63–74.

Bennett, C. H. and Brassard, G. (1984). Quantum Cryptography: Public Key Distribution and Coin Tossing. In Proceedings of IEEE ICCSSP, pages 175–179.

Cao, Y., Zhao, Y., Yu, X., and Zhang, J. (2019). Key on Demand (KoD) for Software-Defined Optical Networks Secured by QKD. JOSAB, 36(3):31–40.

Chen, L., Chen, J., and Chen, Q. (2023). A QKD Routing Scheme for Hybrid-Trusted QKD Network System. Quantum Information Processing, 22:75.

Cisco (2020). Cisco Global Cloud Index: Forecast and Methodology, 2018–2023. White Paper.

Cisco (2023). Building an SRv6 uSID Data Center Fabric with SONiC. Technical Report.

Dervisevic, E., Voznak, M. and Mehic, M. (2024). Large-Scale QKD Network Simulator. JOCN, 16(4):449–462.

ETSI (2019). ETSI GS QKD 014 V1.1.1: QKD; Protocol and Data Format of REST-based Key Delivery API. ETSI.

Filsfils, C. et al. (2018). BGP Prefix Segment in Large-Scale Data Centers. RFC 8670, IETF.

Filsfils, C. et al. (2021). Segment Routing over IPv6 (SRv6) Network Programming. RFC 8986, IETF.

Gisin, N., Ribordy, G., Tittel, W., and Zbinden, H. (2002). Quantum Cryptography. Reviews of Modern Physics, 74(1):145–195.

Greenberg, A. et al. (2009). VL2: A Scalable and Flexible Data Center Network Architecture. In ACM SIGCOMM, pages 51–62.

ID Quantique (2023). Cerberis XG QKD System: Technical Specifications. Product Documentation.

Jain, N., Derksen, C., and Gehring, T. (2023). Quantum Key Distribution for Data Center Security: A Feasibility Study. arXiv:2307.13098.

Lapukhov, P., Premji, A., and Mitchell, J. (2016). Use of BGP for Routing in Large-Scale Data Centers. RFC 7938, IETF.

Lo, H.-K., Ma, X., and Chen, K. (2005). Decoy State Quantum Key Distribution. Physical Review Letters, 94(23):230504.

Mehic, M. et al. (2020). Quantum Key Distribution: A Networking Perspective. ACM Computing Surveys, 53(5):1–41.

OpenQKD (2023). OpenQKD Project: Use Cases and Deployments. https://openqkd.eu/.

Xu, F., Ma, X., Zhang, Q., Lo, H.-K., and Pan, J.-W. (2020). Secure QKD with Realistic Devices. Reviews of Modern Physics, 92(2):025002.