SCOPE: Segurança Quântica Sensível ao Contexto para Aprendizado Federado, Além do Superdimensionamento na Alocação de Chaves QKD

Adriano Maia[1,4], **Isys Sant'Anna** [1,4], **Marcus Freire**[1,4], **Thiago Mello**[1,4], **Bruno Tardiole**[2], **Bruno Guazzelli**[2], **Dionisio Leite**[3], **Maycon Peixoto**[1]

[1]Universidade Federal da Bahia (UFBA)
{adriano.maia, isys.nogueira, thiagomello, maycon.leone}@ufba.br

[2]Universidade Federal de Itajubá (UNIFEI)
{brunokuehne, brunoguazzelli}@unifei.edu.br

[3]Universidade Federal de Mato Grosso do Sul (UFMS)
dionisio.leite@ufms.br

[4]QuIIN – Quantum Industrial Innovation,
Centro de Competência EMBRAPII CIMATEC em Tecnologias Quânticas
marcus.elias@fieb.org.br

Resumo. *A aplicação uniforme de Distribuição Quântica de Chaves (QKD) em Aprendizado Federado assume abundância de recursos criptográficos; contudo, implantações reais enfrentam taxas finitas de geração de chaves e contribuições heterogêneas dos clientes, tornando o superdimensionamento da segurança uma ineficiência sistêmica. Apresentamos o SCOPE, um framework escalável e sensível ao contexto que modela as chaves quânticas como um recurso restrito e aloca dinamicamente a proteção de acordo com o impacto dos clientes, a disponibilidade de chaves e critérios de equidade. Sua política permite proteção proporcional, superando regimes binários de segurança. Avaliado em um ambiente end-to-end que combina treinamento federado real com restrições de rede e QKD, o SCOPE reduz o consumo criptográfico em mais de* $3\times$*, praticamente elimina a escassez de chaves mesmo sob forte restrição e preserva a convergência e a robustez do modelo. Esses resultados demonstram que tratar a segurança quântica como uma variável de controle viabiliza um aprendizado federado quântico seguro, eficiente e escalável.*

Abstract. *Uniform application of Quantum Key Distribution (QKD) in Federated Learning assumes abundant cryptographic resources; however, real deployments face finite key-generation rates and heterogeneous client contributions, making security overprovisioning a systemic inefficiency. We present SCOPE, a scalable context-aware protection framework that models quantum keys as a constrained resource and dynamically allocates security according to client impact, key availability, and fairness. Its policy enables proportional protection, moving beyond binary security regimes. Evaluated in an end-to-end environment combining real federated training with network and QKD constraints, SCOPE reduces cryptographic consumption by over* $3\times$*, virtually eliminates key starvation under severe scarcity, and preserves model convergence and robustness. These findings show that treating quantum security as a control variable enables efficient and scalable quantum-secure federated learning.*

1. Introdução

O *Federated Learning* (FL) permite o treinamento colaborativo de modelos de aprendizado de máquina em ambientes distribuídos sem a necessidade de compartilhamento de dados brutos, sendo amplamente adotado em cenários sensíveis à privacidade, como IoT, aplicações móveis e sistemas ciberfísicos [McMahan et al. 2017, Kairouz et al. 2021, McMahan et al. 2017]. Apesar de seus benefícios, o FL impõe desafios sistêmicos relevantes, incluindo heterogeneidade de dados, limitações de comunicação e a necessidade de proteger as atualizações de modelo trocadas entre clientes e servidor [Li et al. 2020, Kairouz et al. 2021].

A troca periódica de atualizações torna o FL vulnerável a ameaças como espionagem, adulteração de mensagens e ataques de envenenamento conduzidos por participantes maliciosos [Bhagoji et al. 2019, Baruch et al. 2019]. Mecanismos criptográficos são, portanto, essenciais para garantir a segurança do processo. Nesse contexto, a Distribuição Quântica de Chaves (*Quantum Key Distribution* – QKD) destaca-se por oferecer garantias de segurança fundamentadas em princípios da mecânica quântica, possibilitando a geração de chaves secretas com confidencialidade teoricamente incondicional [Gisin et al. 2002, Lo et al. 2014, Freire et al. 2025].

Entretanto, a QKD é um recurso inerentemente limitado, com taxas finitas de geração de chaves, alto custo de infraestrutura e capacidade restrita de armazenamento [Gisin et al. 2002, Lo et al. 2014]. Essas limitações tornam inviável sua aplicação indiscriminada em todas as rodadas e clientes de um sistema de Aprendizado Federado em larga escala, podendo resultar em desperdício de recursos e eventos recorrentes de escassez. Diante disso, este trabalho investiga como alocar segurança quântica [Maia et al. 2025, Peixoto 2024] em Federated Learning de forma eficiente, tratando a QKD como um recurso alocável e dinâmico, cuja utilização deve ser ajustada ao longo do tempo e entre clientes para preservar o desempenho do aprendizado e a eficiência do sistema.

Neste artigo, propomos uma política de proteção escalável e sensível ao contexto para Aprendizado Federado, que realiza a alocação dinâmica, seletiva e proporcional de recursos de QKD. A política considera simultaneamente o estado de escassez das chaves disponíveis, o impacto relativo das atualizações de cada cliente no modelo global e critérios de equidade no uso dos recursos. Para avaliar a proposta, desenvolvemos um *framework* experimental que combina treinamento federado real com uma camada analítica de simulação de comunicação e disponibilidade de QKD. Os resultados demonstram que a abordagem proposta mantém desempenho competitivo de aprendizado ao mesmo tempo em que reduz significativamente o consumo de chaves quânticas quando comparada a estratégias tradicionais.

As principais contribuições deste trabalho são três. Primeiro, introduzimos um modelo que trata a segurança quântica como um recurso escasso e alocável no contexto de Federated Learning. Segundo, propomos uma política de proteção escalável e sensível ao contexto que aloca recursos de QKD de forma dinâmica, seletiva e proporcional, considerando impacto das atualizações, escassez e equidade. Por fim, desenvolvemos um *framework* experimental *end-to-end* que combina treinamento federado real com simulação de comunicação e disponibilidade de QKD, permitindo uma avaliação sistemática sob diferentes cenários.

2. Trabalhos Relacionados

O FL sob restrições sistêmicas tem sido extensivamente explorado na literatura, com ênfase primária em desafios de infraestrutura clássica, como a heterogeneidade estatística dos dados (non-IID), limitações de largura de banda e escalabilidade massiva [Li et al. 2020, Kairouz et al. 2021]. Para mitigar os custos de rede e a latência inerente a esses cenários, estratégias como a seleção parcial de clientes [McMahan et al. 2017], a compressão de vetores de atualização e a redução da frequência de agregação se tornaram padrões de otimização. No entanto, essas abordagens compartilham uma limitação estrutural crítica: elas otimizam a eficiência de transmissão assumindo, implicitamente, que os canais de comunicação dispõem de mecanismos de segurança homogêneos, onipresentes e custo sem operacional.

Paralelamente à otimização de recursos se dedica à robustez da privacidade em FL, empregando técnicas como Agregação Segura [Bonawitz et al. 2019], Privacidade Diferencial [Ponomareva et al. 2023, Truex et al. 2019] e Agregação Segura para blindar o conteúdo das atualizações contra adversários externos e internos [Lyu et al. 2020, Puthal et al. 2025]. Embora essas soluções ofereçam garantias teóricas sólidas de confidencialidade, elas operam predominantemente sob uma lógica de aplicação uniforme e contínua, pressupondo infraestruturas capazes de suportar o overhead computacional e de comunicação constante que tais protocolos exigem.

Nesse contexto, a Distribuição de Chaves Quânticas (QKD) se destaca por oferecer garantias de segurança fundamentadas na física, possibilitando a confidencialidade incondicional [Gisin et al. 2002, Lo et al. 2014]. Contudo, a integração de QKD em FL enfrenta barreiras físicas que a literatura recente frequentemente subestima. Propostas contemporâneas de arquiteturas seguras tendem a modelar a camada de segurança como um provedor de serviço idealizado ou focar exclusivamente na robustez algorítmica [Sundaramurthy et al. 2025, Puthal et al. 2025], assumindo implicitamente taxas de geração de chaves suficientes para cobrir todo o tráfego de treinamento.

Na prática, a QKD é um recurso inerentemente limitado, com taxas finitas de geração e capacidade restrita de armazenamento nos pools locais [Lo et al. 2014]. A suposição de abundância leva ao superdimensionamento da segurança, resultando em desperdício de entropia em atualizações de baixo impacto e, criticamente, em esgotamento de chaves nos momentos de pico. Diferente das abordagens listadas na Tabela 1, este trabalho visa tratar a segurança quântica não como uma constante binária, mas como um recurso escasso, alocável e dinâmico.

Tabela 1. Trabalhos relacionados sobre segurança e eficiência em FL

Autor(es)	FL	Segurança	Adaptativo	Escassez	Equidade
McMahan et al. (2017)	✓	✗	✗	✗	✗
Bonawitz et al. (2017)	✓	✓	✗	✗	✗
Ponomareva et al. (2023)	✓	✓	✗	✗	✗
Kairouz et al. (2021)	✓	✓	✗	✗	✗
Truex et al. (2019)	✓	✓	✓	✗	✗
Lyu et al. (2020)	✓	✓	✗	✗	✗
Puthal et al. (2025)	✓	✗	✓	✗	✗
Sundaramurthy et al. (2025)	✓	✓	✓	✗	✗
SCOPE	✓	✓	✓	✓	✓

3. SCOPE – Scalable COntext-aware Protection Environment

O framework do sistema proposto e o fluxo de operação por rodada são detalhados na Figura 1. O diagrama ilustra a integração entre o ambiente de Aprendizado Federado (FL) e a infraestrutura de Distribuição de Chaves Quânticas (QKD), enfatizando o papel do algoritmo de Segurança Quântica Sensível ao Contexto. Diferente de abordagens tradicionais de superdimensionamento, o módulo proposto atua como um controlador dinâmico: ele processa sinais de contexto (estado da rede, relevância da atualização do cliente e nível do pool de chaves) para determinar a fração de proteção q_i aplicada a cada cliente. Esse mecanismo permite uma transição fluida entre a comunicação clássica e a protegida por one-time pad via QKD, otimizando o consumo do recurso escasso sem comprometer a integridade da agregação global.

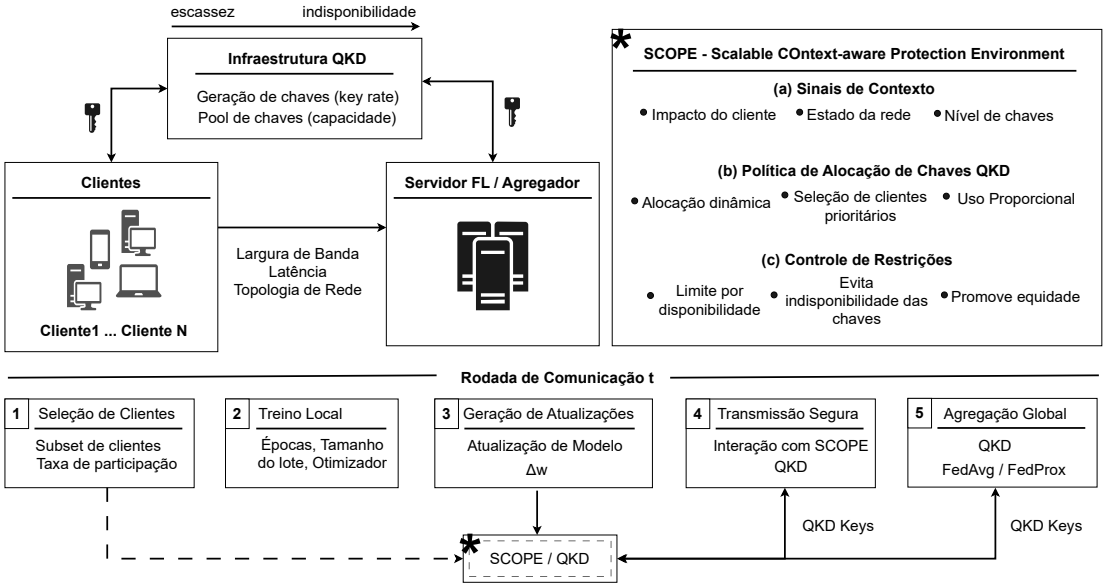


Figura 1. Visão geral do SCOPE e sua integração ao pipeline de *Federated Learning*. O framework atua como uma camada decisória que aloca dinamicamente proteção via QKD ciente do contexto operacional.

A arquitetura mantem separadas as partes sobre o aprendizado, comunicação e controle criptográfico, posicionando o algoritmo proposto como uma camada decisória transversal ao pipeline federado. Ao operar no nível da rodada, o controlador ajusta continuamente o grau de proteção em resposta às condições operacionais, evitando tanto o subdimensionamento, que comprometeria a confidencialidade, quanto o superdimensionamento, que induz consumo criptográfico desnecessário e eleva o risco de escassez. Como resultado, o sistema passa a operar em um regime adaptativo, no qual segurança e desempenho deixam de competir por recursos e passam a ser co-otimizados. Essa integração transforma a infraestrutura QKD de um componente passivo em um elemento ativo de orquestração do treinamento, permitindo sustentar estabilidade estatística mesmo sob taxas limitadas de geração de chaves.

3.1. Provisionamento Sensível ao Contexto de Segurança Quântica

A provisão de segurança quântica em sistemas de aprendizado federado pode ser naturalmente formulada como um problema de alocação de recursos sob restrições físicas. Diferentemente de modelos que assumem disponibilidade irrestrita de chaves ou que impõem proteção uniforme, tratamos o uso de QKD como uma variável de controle contínua cuja decisão deve equilibrar consumo criptográfico e utilidade estatística.

Considere uma rodada de treinamento r com o conjunto de clientes selecionados $\mathcal{S}^{(r)}$. Para cada cliente $i \in \mathcal{S}^{(r)}$, definimos uma fração de proteção $q_i^{(r)} \in [0,1]$, correspondente à proporção do payload protegida via QKD. Cada cliente mantém um *pool* local de chaves $\Pi_i = (B_i, B_i^{\max})$, onde B_i representa o estoque disponível e $B_i^{\max}$ sua capacidade máxima. Adicionalmente, associamos um escore de impacto estatístico I_i, que estima a relevância da atualização local para o modelo global, e um consumo histórico U_i, empregado como mecanismo de regularização para evitar concentração do recurso criptográfico.

Sob essa formulação, a provisão de segurança consiste em determinar o vetor de alocação $\mathbf{q}^{(r)} = \{q_i^{(r)}\}_{i \in \mathcal{S}^{(r)}}$, que maximize a utilidade esperada do treinamento enquanto respeita as limitações impostas pela infraestrutura quântica. Para contextualizar a proposta, consideramos quatro políticas de referência que delimitam o espaço de decisões. Essas estratégias são formalizadas no Algoritmo 1, que sintetiza diferentes regimes de provisão criptográfica sob distintos graus de disponibilidade de chaves.

Algoritmo 1 Políticas de Provisionamento de Segurança Quântica

Entrada: Clientes selecionados $\mathcal{S}^{(r)}$
Saída: Vetor de proteção $\mathbf{q}^{(r)}$
CLASSICAL:
$\mathbf{q}^{(r)} \leftarrow \mathbf{0}$
ALL_QKD:
$\mathbf{q}^{(r)} \leftarrow \mathbf{1}$
STATIC_SPLIT:
Selecione subconjunto fixo $\mathcal{K} \subseteq \mathcal{S}^{(r)}$
$q_i^{(r)} \leftarrow \mathbb{1}[i \in \mathcal{K}]$
RANDOM:
$q_i^{(r)} \sim \text{Bernoulli}(p)$
SCOPE:
$\mathbf{q}^{(r)} \leftarrow \text{SCOPE}(\mathcal{S}^{(r)})$
return $\mathbf{q}^{(r)}$

As políticas CLASSICAL e ALL_QKD estabelecem limites inferior e superior de consumo, respectivamente, enquanto STATIC_SPLIT e RANDOM introduzem mecanismos rudimentares de contenção. Contudo, por desconsiderarem tanto o estado global do sistema quanto a heterogeneidade estatística dos clientes, essas estratégias tendem a converter disponibilidade de chaves diretamente em consumo, operando frequentemente fora da fronteira eficiente. Já o SCOPE é formalizado no Algoritmo 2, uma política de provisão criptográfica sob restrições responsável por determinar o vetor de alocação $\mathbf{q}^{(r)} = \{q_i^{(r)}\}_{i \in \mathcal{S}^{(r)}}$, com $q_i^{(r)} \in [0,1]$, que regula a fração do payload protegida via QKD na rodada r.

Seja $\mathcal{S}^{(r)}$ o conjunto de clientes selecionados. Cada cliente i mantém um *pool* local $\Pi_i = (B_i, B_i^{\max})$, onde B_i representa o estoque disponível e $B_i^{\max}$ sua capacidade máxima. Associam-se ainda um escore de impacto estatístico I_i e um consumo acumulado

Algoritmo 2 SCOPE: Provisionamento Sensível ao Contexto

Entrada: clientes selecionados $\mathcal{S}^{(r)}$; impactos I_i; pools $(B_i, B_i^{\max})$; consumo histórico U_i; parâmetros $q_{\text{base}}, \rho, \beta, \gamma$; payload L
Saída: vetor de proteção $\mathbf{q}^{(r)}$
Inicializar $\mathbf{q}^{(r)} \leftarrow \mathbf{0}$
Estimar pressão de escassez $s^{(r)}$ a partir dos níveis médios dos pools (controlada por β)
Selecionar clientes prioritários $\mathcal{E}^{(r)} \subseteq \mathcal{S}^{(r)}$ (Top-ρ por impacto)
for cada $i \in \mathcal{E}^{(r)}$ **do**
    Calcular proteção base proporcional ao impacto: $q_i^{(r)} \leftarrow q_{\text{base}} \cdot s^{(r)} \cdot \tilde{I}_i$
end for
Calcular consumo médio dos prioritários $\bar{U}$
for cada $i \in \mathcal{E}^{(r)}$ **do**
    Aplicar fator de equidade: $q_i^{(r)} \leftarrow q_i^{(r)} \cdot \exp\big(-\gamma \cdot U_i/\bar{U}\big)$
end for
for cada $i \in \mathcal{E}^{(r)}$ **do**
    Impor viabilidade pelo pool local: $q_i^{(r)} \leftarrow \min\big(q_i^{(r)},\, B_i/L\big)$
end for
return $\mathbf{q}^{(r)}$

U_i. O vetor $\mathbf{q}^{(r)}$ é obtido a partir de três sinais sistêmicos: disponibilidade criptográfica, relevância estatística e regularização de consumo. O grau de pressão sobre a infraestrutura é estimado por:

$$s^{(r)} = \left(\frac{1}{|\mathcal{S}^{(r)}|} \sum_{i \in \mathcal{S}^{(r)}} \frac{B_i}{B_i^{\max}} \right)^{\beta},$$

onde $\beta > 0$ controla a sensibilidade à escassez. Seja $\mathcal{E}^{(r)} = \text{Top}_\rho(\mathcal{S}^{(r)}, I)$ o subconjunto prioritário correspondente à fração superior ρ dos clientes ordenados por impacto. Para cada $i \in \mathcal{E}^{(r)}$, define-se a alocação inicial como $q_i^{(r)} = q_{\text{base}}\, s^{(r)}\, \tilde{I}_i$, onde $\tilde{I}_i$ denota o impacto normalizado. A fim de evitar concentração do recurso criptográfico, introduz-se um fator de equidade $\phi_i = \exp\big(-\gamma \frac{U_i}{\bar{U}}\big)$, com $\bar{U} = \frac{1}{|\mathcal{E}^{(r)}|} \sum_{j \in \mathcal{E}^{(r)}} U_j$, resultando na alocação regularizada $q_i^{(r)} \leftarrow q_i^{(r)} \phi_i$. Impõe-se, por fim, a restrição de viabilidade $q_i^{(r)} \leq \frac{B_i}{L}$, onde L representa o tamanho do payload em bits. O vetor final $\mathbf{q}^{(r)}$ corresponde à projeção da alocação no conjunto factível definido pela capacidade dos pools. O procedimento completo é descrito no Algoritmo 2.

O SCOPE induz um regime de provisão adaptativo no qual decisões de segurança emergem da interação entre pressão criptográfica e relevância estatística, deslocando o sistema para uma região operacional próxima à fronteira eficiente entre consumo e utilidade. Além disso, a política estrutura o processo decisório de provisionamento criptográfico a cada rodada de treinamento ao combinar sinais sistêmicos e estatísticos. Inicialmente, avalia-se o nível de escassez dos recursos de QKD e classificam-se os clientes selecionados conforme seu impacto esperado no aprendizado global. Em seguida, calcula-se uma fração proporcional de proteção para os clientes prioritários, ajustando a alocação com base em critérios de equidade e viabilidade operacional. A decisão resultante é então aplicada durante a comunicação das atualizações locais, permitindo que o grau de proteção acompanhe dinamicamente as condições do sistema.

Esse comportamento é sustentado por quatro princípios complementares: (i) **consciência de escassez**, que adapta o uso de QKD à disponibilidade média de chaves, evitando exaustão prematura; (ii) **seletividade**, ao priorizar clientes com maior re-

levância estatística; (iii) **proporcionalidade**, que viabiliza níveis contínuos e até parciais de proteção em uma mesma rodada; e (iv) **equidade**, ao incorporar o histórico de consumo para impedir a concentração do recurso criptográfico. Em conjunto, esses princípios conduzem o sistema a um regime adaptativo no qual segurança e eficiência são tratadas como variáveis co-dependentes.

Para orientar a seletividade da política, associamos a cada cliente i um *score* de impacto $I_i^{(r)}$ na rodada r. Esse valor é calculado com base na norma da diferença entre os parâmetros do modelo local antes e após o treinamento, refletindo a magnitude da contribuição do cliente para a atualização global. Ao longo das rodadas, o impacto é suavizado por meio de uma média móvel exponencial, permitindo capturar tendências sem reagir excessivamente a flutuações pontuais.

Em cada rodada, a política SCOPE calcula, para cada cliente selecionado, uma fração $q_i^{(r)} \in [0, 1]$ do payload que deve ser protegida por QKD. Essa fração é determinada pela combinação do impacto normalizado do cliente, do nível médio de disponibilidade de chaves e de um fator de equidade que penaliza clientes com alto consumo histórico.

A fração calculada é posteriormente limitada pela quantidade efetivamente disponível de chaves no *pool* do cliente, garantindo que a alocação seja sempre factível. Caso os recursos sejam insuficientes, a política reduz automaticamente o nível de proteção ou desativa o uso de QKD para aquele cliente na rodada corrente, evitando falhas no processo de comunicação.

3.2. Exemplo Ilustrativo

Para oferecer uma visão intuitiva do mecanismo decisório das políticas de provisionamento, apresentamos na Figura 2 um exemplo simplificado de uma única rodada de treinamento sob escassez criptográfica. Considera-se um pool limitado de 200 kb e cinco clientes com diferentes níveis de demanda e impacto estatístico. Embora não represente a escala completa do sistema, o cenário sintetiza o dilema central do provisionamento quântico: determinar como distribuir um recurso escasso sem comprometer a continuidade operacional do aprendizado federado.

Observa-se que políticas rígidas, como *ALL_QKD*, tendem a concentrar recursos nos primeiros clientes até a exaustão do pool, resultando em bloqueios e baixa participação. Estratégias parcialmente estáticas podem inclusive exceder o orçamento disponível, enquanto abordagens aleatórias introduzem variabilidade operacional e não oferecem garantias de eficiência. Em contraste, o SCOPE adapta o nível de proteção ao impacto dos clientes e à disponibilidade de chaves, permitindo o uso parcial de QKD quando necessário. Como resultado, a política mantém mais clientes ativos, reduz eventos de *starvation* e utiliza o orçamento criptográfico de forma mais disciplinada. Esse comportamento antecipa os resultados quantitativos das seções seguintes e evidencia o princípio fundamental da proposta: transformar a segurança quântica de uma restrição rígida em uma variável de controle alinhada à utilidade do aprendizado.

4. Configuração dos Experimentos

Os experimentos foram conduzidos em um framework de simulação end-to-end que integra treinamento federado real com uma camada analítica de comunicação e disponibilidade de chaves quânticas. A Tabela 2 sintetiza os principais parâmetros do ambiente

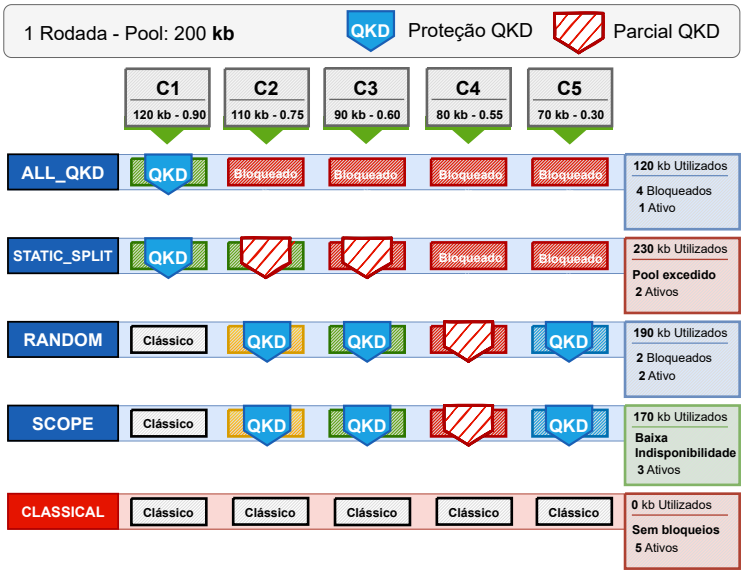


Figura 2. Exemplo Ilustrativo com pool limitado (200 kb).As cores indicam o nível de proteção aplicado a cada cliente: cinza representa comunicação clássica (sem QKD); tons progressivos (amarelo, verde e azul) denotam frações crescentes do payload protegidas via QKD; o padrão listrado indica proteção parcial sob restrição criptográfica; e vermelho sinaliza clientes bloqueados por esgotamento do pool.

experimental, organizando as dimensões de aprendizado, dados, rede e infraestrutura criptográfica consideradas neste estudo.

Tabela 2. Principais parâmetros do ambiente experimental.

Categoria	Parâmetro	Valor
Aprendizado Federado	Algoritmos	FedAvg, FedProx
	Dataset	MNIST
	Número de clientes	50
	Clientes por rodada	20%
	Rodadas de treinamento	200
	Taxa de aprendizado	0.01
Dados	Particionamento	Dirichlet ($\alpha = 0.3$)
	Cenário estatístico	Não-IID
	Amostras mínimas por cliente	Garantidas
Rede	Topologias	STAR, RING, TWO_HOP
	Largura de banda	Parametrizável
	Latência	Parametrizável
	Modelo de comunicação	Analítico
Infraestrutura QKD	Taxa média de geração	2×10^5 bps
	Capacidade do pool	2×10^7 bits
	Reabastecimento	Contínuo entre rodadas
Execução	Políticas avaliadas	CLASSICAL, ALL_QKD, STATIC_SPLIT, RANDOM, SCOPE
	Controle estatístico	Sementes fixas e múltiplas execuções

O ambiente suporta múltiplos algoritmos de aprendizado federado, incluindo FedAvg e FedProx, bem como o dataset de referência MNIST, amplamente utilizado para avaliação de sistemas distribuídos de aprendizado. Em cada execução, consideramos uma população de 50 clientes, dos quais 20% são selecionados por rodada ao longo de 200 iterações de treinamento, utilizando lotes de tamanho 32, uma época local e taxa de

aprendizado 0.01. Para capturar heterogeneidade estatística, o particionamento dos dados segue uma distribuição de Dirichlet com parâmetro $\alpha = 0.3$, produzindo cenários não-IID representativos de implantações reais. Além disso, impomos um número mínimo de amostras por cliente para evitar participantes vazios e garantir estabilidade numérica durante o treinamento federado.

A infraestrutura de rede é modelada por um simulador parametrizável capaz de representar diferentes topologias (*STAR*, *RING* e *TWO_HOP*), além de variações de largura de banda e latência. Cada cliente mantém um *pool* local de chaves QKD cuja taxa média de geração é configurada em torno de 2×10^5 bps, com heterogeneidade controlada e capacidade máxima de 2×10^7 bits; as chaves são continuamente reabastecidas entre rodadas para refletir a natureza estocástica da produção quântica. Esse modelo permite avaliar explicitamente regimes de escassez criptográfica e seus efeitos sobre o treinamento. As políticas de segurança, CLASSICAL, ALL_QKD, STATIC_SPLIT, RANDOM e SCOPE, são instanciadas sob os mesmos parâmetros operacionais, variando apenas os hiperparâmetros específicos de alocação, como fração base, priorização top-k, sensibilidade à escassez e fator de equidade.

O modelo de ameaça assume um ambiente de *Federated Learning* com servidor confiável, porém suscetível a clientes internos maliciosos que realizam ataques de *model poisoning* do tipo *sign-flip*, enviando atualizações manipuladas para degradar o modelo global. A comunicação é protegida por mecanismos criptográficos com chaves distribuídas via QKD, garantindo segurança contra adversários externos; contudo, essa proteção não valida a semântica das atualizações, permitindo que ataques internos ocorram independentemente do canal seguro. O escopo exclui comprometimento do servidor, ataques à infraestrutura de QKD, inferência de dados e defesas robustas contra envenenamento, pois o objetivo é isolar e analisar como o provisionamento de segurança quântica interage com perturbações internas no processo de aprendizado.

5. Resultados

Esta seção analisa os resultados experimentais com o objetivo de compreender as decisões de provisionamento criptográfico.

5.1. Provisionamento e Escassez de Recursos Quânticos

Para compreender como restrições criptográficas influenciam o comportamento do aprendizado federado, avaliamos o sistema sob diferentes taxas de geração de chaves quânticas, modelando um espectro operacional que varia de escassez severa a abundância relativa. Consideramos $\bar{R}_k \in \{50, 200, 800\}$ kbps e um *pool* proporcional ($B_{\max} = 100\bar{R}_k$), permitindo observar não apenas a suficiência do serviço criptográfico, mas principalmente a capacidade de adaptação das políticas quando a disponibilidade de chaves passa a atuar como restrição estrutural do sistema.

A Figura 3 apresenta uma visão integrada desse comportamento por meio de três perspectivas complementares: (i) o consumo acumulado de QKD ao longo dos regimes operacionais, (ii) a pressão exercida sobre o orçamento criptográfico, medida pelo acúmulo de requisições pendentes, e (iii) o consumo agregado por política. Em conjunto, esses indicadores permitem distinguir políticas que apenas convertem capacidade adicional em gasto daquelas capazes de transformar escassez em disciplina operacional.

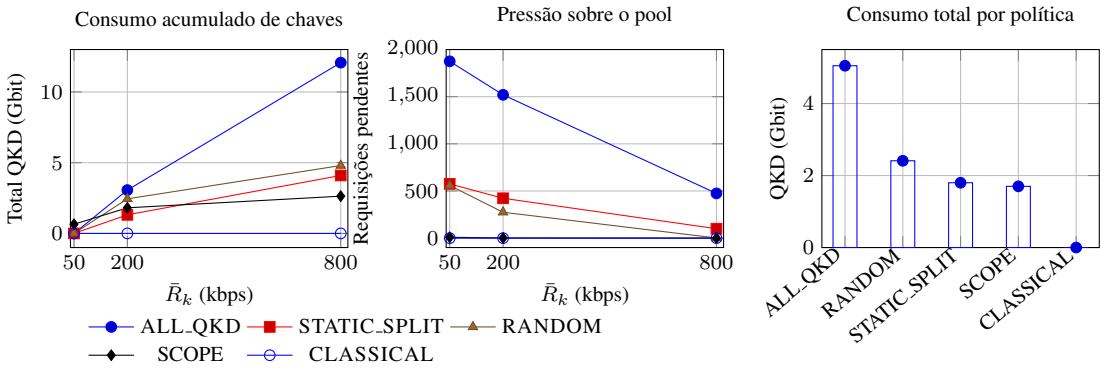


Figura 3. Impacto da escassez de chaves quânticas.

Os resultados evidenciam uma vantagem estrutural da política adaptativa SCOPE. Enquanto abordagens rígidas escalam o consumo quase linearmente com o aumento da oferta, o ALL_QKD atinge aproximadamente 12.07 Gbit no tier de 800 kbps, ao passo que o SCOPE limita esse valor a cerca de 2.63 Gbit, uma redução superior a 3× no uso do recurso criptográfico. Essa diferença torna-se ainda mais expressiva no consumo agregado, onde a política adaptativa utiliza apenas 1.70 Gbit, contra 5.05 Gbit do provisionamento total, evidenciando ganhos substanciais de eficiência sistêmica.

A economia de chaves traduz-se diretamente em maior estabilidade operacional. Sob escassez severa (50 kbps), o ALL_QKD acumula 1875 requisições pendentes, caracterizando um regime persistente de contenção, enquanto o SCOPE mantém apenas 9.17, praticamente eliminando o backlog. Observa-se ainda que ampliar a oferta não corrige ineficiências estruturais: políticas estáticas continuam formando filas relevantes mesmo em regimes mais favoráveis, sugerindo que o simples superdimensionamento do orçamento criptográfico pode mascarar desperdícios operacionais. Em contraste, ao alinhar dinamicamente decisões de proteção à capacidade física do canal quântico, o SCOPE promove um uso sustentável das chaves e converte escassez em um mecanismo de controle sistêmico, reforçando simultaneamente eficiência e estabilidade.

5.2. Convergência do Modelo

Como as curvas absolutas de acurácia e perda tendem a se sobrepor em regimes próximos à convergência, adotamos uma visualização baseada em diferenças relativas ao cenário clássico (Figura 4). Essa representação em Δ funciona como uma lente analítica, ampliando variações que seriam visualmente imperceptíveis e permitindo avaliar com maior sensibilidade se as políticas de provisionamento introduzem desvios sistemáticos na trajetória de aprendizado.

Observa-se que os desvios em relação ao cenário clássico permanecem limitados e não apresentam tendência acumulativa ao longo do treinamento. Após a fase transitória inicial, caracterizada por maior variabilidade, as curvas se estabilizam rapidamente em torno de zero, indicando ausência de viés induzido pelas políticas de proteção. Na acurácia, as flutuações permanecem tipicamente abaixo de meio ponto percentual, enquanto as diferenças na perda convergem para uma faixa estreita compatível com o ruído da otimização estocástica. O comportamento do SCOPE é particularmente expressivo: mesmo operando sob priorização adaptativa, sua trajetória oscila simetricamente ao re-

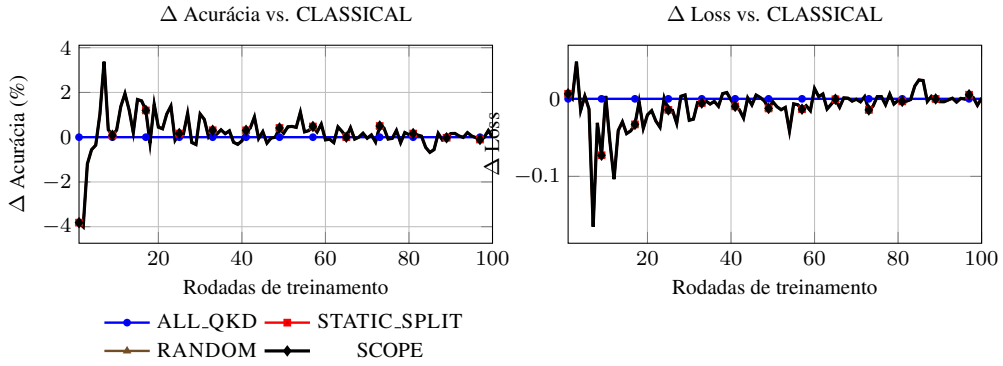


Figura 4. Diferença em relação ao cenário clássico (CLASSICAL) ao longo das rodadas.

dor do baseline, sem evidenciar degradação persistente nem atraso de convergência. Em termos práticos, isso demonstra que a política preserva a solução estatística do problema de aprendizado, sugerindo que restrições criptográficas, quando tratadas de forma adaptativa, impactam predominantemente a operação do sistema, e não a qualidade do modelo resultante.

5.3. Equidade e Escassez na Alocação

Além de preservar estabilidade e eficiência de aprendizado, uma política de provisionamento criptográfico precisa garantir que o processo colaborativo permaneça operacionalmente viável ao longo do tempo. Em ambientes federados sujeitos à escassez de chaves, decisões de proteção podem introduzir efeitos colaterais relevantes, como bloqueios recorrentes de clientes e episódios de *starvation*, nos quais atualizações deixam de ocorrer por indisponibilidade de recursos. Para caracterizar esse comportamento, analisamos conjuntamente três dimensões complementares: (i) o índice de Jain (J), que mede a uniformidade da participação; (ii) o percentual de clientes bloqueados; e (iii) o volume acumulado de eventos de *starvation*. Essa combinação permite avaliar não apenas a justiça distributiva, mas também a capacidade do sistema de sustentar continuidade operacional sob restrições criptográficas. Dessa forma, a Figura 5 mostra um trade-off estrutural entre equidade estatística e viabilidade operacional.

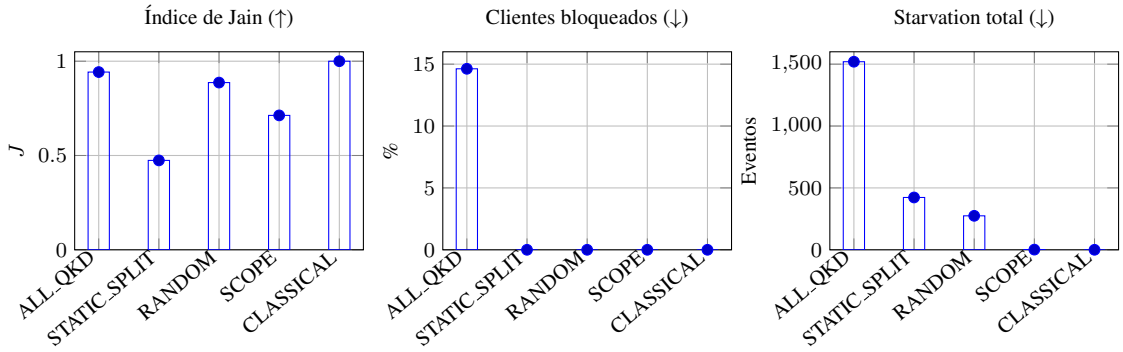


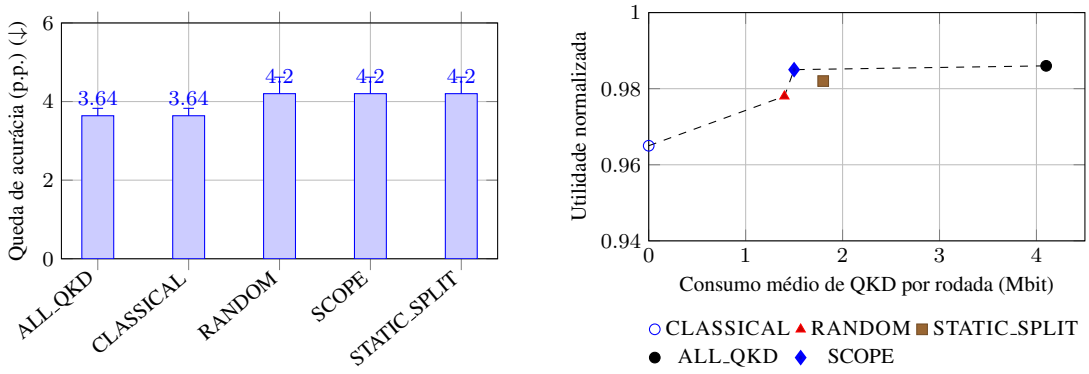
Figura 5. Equidade e viabilidade operacional sob orçamento quântico limitado.

O ALL_QKD apresenta alta uniformidade de participação ($J \approx 0.94$), aproximando-se do cenário clássico ($J = 1$), porém à custa de bloqueios frequentes e

do maior nível de *starvation* observado. Esse comportamento indica que políticas criptograficamente inflexíveis podem preservar equilíbrio distributivo apenas restringindo o conjunto efetivo de colaboradores, comprometendo a fluidez do treinamento. No extremo oposto, o SCOPE praticamente elimina eventos de *starvation* e evita bloqueios, mantendo todos os clientes potencialmente ativos. Embora essa estratégia resulte em menor uniformidade ($J \approx 0.71$), ela favorece continuidade operacional e reduz o risco de interrupções sistêmicas. Em conjunto, os resultados sugerem que maximizar justiça distributiva nem sempre conduz ao regime mais eficiente: ao internalizar explicitamente a escassez no processo decisório, o SCOPE estabelece um ponto de equilíbrio entre diversidade estatística e sustentabilidade do treinamento federado.

5.4. Robustez e Eficiência sob Restrições Criptográficas

A avaliação do provisionamento adaptativo de chaves deve considerar não apenas sua viabilidade operacional, mas também seus efeitos sobre a robustez adversarial e o ponto de operação do sistema. A Figura 6 sintetiza essas duas dimensões complementares: enquanto a subfigura 6a quantifica o impacto de um ataque persistente de envenenamento na qualidade do modelo, a subfigura 6b caracteriza a relação entre consumo criptográfico e utilidade global.



(a) Queda de acurácia sob ataque persistente.

(b) Mapa de eficiência segurança–desempenho.

Figura 6. Robustez do aprendizado e eficiência criptográfica sob diferentes políticas de provisão.

A subfigura 6a apresenta a queda de acurácia em pontos percentuais, definida como a diferença entre a acurácia final no cenário sem ataque e aquela observada sob envenenamento, mantendo-se fixas as demais condições experimentais. Observa-se que a degradação induzida pelo ataque permanece no mesmo regime para todas as políticas, com valores médios entre 3.64 e 4.20 p.p. Em particular, ALL_QKD e CLASSICAL registram quedas de 3.64 p.p., enquanto SCOPE, juntamente com RANDOM e STATIC_SPLIT, apresenta aproximadamente 4.20 p.p. A proximidade entre as barras indica que a vulnerabilidade é predominantemente governada pelo efeito estatístico do ataque sobre o mecanismo de agregação, e não pelo regime de provisão criptográfica. Esse resultado evidencia que o SCOPE não introduz penalidade adversarial relevante ao modificar a alocação de QKD.

A subfigura 6b evidencia o posicionamento das políticas no espaço segurança–desempenho. Estratégias extremas operam fora da região eficiente: CLASSI-

CAL minimiza o consumo à custa da ausência de proteção robusta, enquanto ALL_QKD impõe o maior dispêndio criptográfico com ganhos marginais de utilidade, caracterizando retornos decrescentes. Políticas intermediárias, como RANDOM e STATIC_SPLIT, aproximam-se da fronteira, mas ainda carregam ineficiências decorrentes da alocação indiferenciada de chaves. Em contraste, o SCOPE prover utilidade praticamente equivalente ao cenário integralmente protegido com cerca de 65% menos consumo que o ALL_QKD. Esse resultado indica que a segurança adaptativa preserva a estabilidade do aprendizado ao mesmo tempo em que desloca o sistema para um regime operacional mais eficiente.

6. Conclusão

Este trabalho aborda o papel da segurança quântica em *Federated Learning* ao modelá-la não como uma garantia uniforme, mas como um recurso físico limitado que deve ser estrategicamente orquestrado ao longo do treinamento. Por meio do SCOPE – (*Scalable COntext-aware Protection Environment*), demonstramos que o provisionamento sensível ao contexto desloca o sistema para uma região operacional próxima à fronteira eficiente entre consumo criptográfico e utilidade do aprendizado. A política adaptativa reduziu o consumo de QKD em mais de 3× quando comparada ao provisionamento integral, ao mesmo tempo em que praticamente eliminou o acúmulo de requisições. Apesar dessa economia substancial, a convergência permaneceu estável e a robustez adversarial foi preservada, apresentando degradação comparável às demais políticas. Esses resultados indicam que a alocação adaptativa pode mitigar a escassez e evitar desperdícios estruturais, transformando a própria infraestrutura QKD em um mecanismo ativo de controle sistêmico.

Disponibilidade de Artefatos

Em aderência aos princípios da Ciência Aberta, o código-fonte e o dataset utilizados neste trabalho podem ser acessados em: https://github.com/adianohum/SCOPE.

Agradecimentos

Este trabalho foi parcialmente financiado pelo projeto QuIIN "Integração CV-QKD com Redes Clássicas", apoiado pelo QuIIN – *Quantum Industrial Innovation*, Centro de Competência EMBRAPII CIMATEC em Tecnologias Quânticas. O apoio contou com recursos financeiros do programa PPI IoT/Manufatura 4.0, no âmbito da chamada MCTI nº 053/2023, estabelecida com a EMBRAPII. Este estudo também foi financiado, em parte, pela Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001, e pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), Brasil, sob a concessão nº 403231/2023-0.

Referências

Baruch, G., Baruch, M., and Goldberg, Y. (2019). A little is enough: Circumventing defenses for distributed learning. In *Advances in Neural Information Processing Systems (NeurIPS)*.

Bhagoji, A. N., Chakraborty, S., Mittal, P., and Calo, S. (2019). Analyzing federated learning through an adversarial lens. In *Proceedings of the 36th International Conference on Machine Learning (ICML)*.

Bonawitz, K., Eichner, H., Grieskamp, W., et al. (2019). Towards federated learning at scale: System design. In *Proceedings of the 2nd SysML Conference*.

Freire, M., Mello, T. L., Sant'Anna, I., Maia, A., Moreira, R., Rivelino, R., and Peixoto, M. (2025). Rana: Uma abordagem híbrida para qkd bb84 com expansão e encapsulamento de chave. In *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)*, pages 938–951. SBC.

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

Kairouz, P., McMahan, H. B., Avent, B., et al. (2021). Advances and open problems in federated learning. *Foundations and Trends® in Machine Learning*, 14(1–2):1–210.

Li, T., Sahu, A. K., Talwalkar, A., and Smith, V. (2020). Federated optimization in heterogeneous networks. In *Proceedings of Machine Learning and Systems (MLSys)*.

Lo, H.-K., Curty, M., and Qi, B. (2014). Secure quantum key distribution. *Nature Photonics*, 8(8):595–604.

Lyu, L., Yu, H., Ma, X., et al. (2020). Privacy and robustness in federated learning: Attacks and defenses. *IEEE Transactions on Neural Networks and Learning Systems*.

Maia, A., Freire, M., Mello, T., Rodrigues-Filho, R., Almeida, E., Prazeres, C., Figueiredo, G., and Peixoto, M. (2025). Q-edge: Leveraging quantum computing for enhanced software engineering in vehicular networks. In *Proceedings of the 40th ACM/SIGAPP Symposium on Applied Computing*, pages 1457–1467.

McMahan, H. B., Moore, E., Ramage, D., Hampson, S., and y Arcas, B. A. (2017). Communication-efficient learning of deep networks from decentralized data. In *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS)*.

Peixoto, M. L. M. (2024). Quantum edge computing for data analysis in connected autonomous vehicles. In *2024 IEEE Symposium on Computers and Communications (ISCC)*, pages 1–6. IEEE.

Ponomareva, N., Hazimeh, H., Kurakin, A., Xu, Z., Denison, C., McMahan, H. B., Vassilvitskii, S., Chien, S., and Thakurta, A. G. (2023). How to dp-fy ml: A practical guide to machine learning with differential privacy. *Journal of Artificial Intelligence Research*, 77:1113–1201.

Puthal, D., Yeun, C. Y., Sharma, P. K., and Ding, Z. (2025). Privacy-preserving federated learning for the edge-intelligent 6g ecosystem. *IEEE Communications Standards Magazine*.

Sundaramurthy, A., Kathavarayan, R., Raju, K. K., Dayalan, S. P., Mohan, J., and Sivakolundu, V. P. (2025). Quantum-secured federated learning for privacy-preserving and adaptive attack detection in 6g iot. In *Secure Communication for the 6G and the Internet of Things Networks*, pages 253–276. CRC Press.

Truex, S., Baracaldo, N., Anwar, A., et al. (2019). A hybrid approach to privacy-preserving federated learning. In *Proceedings of the 12th ACM Workshop on Artificial Intelligence and Security (AISec)*.