QML Federado em uma Rede BQC: Impactos do Gerenciamento de Recursos

Andrey Silva da Silva[1], David Tavares[1], Diego Abreu[1,2], Antônio Abelém[1]

Universidade Federal do Pará (UFPA)

[2]Rede Nacional de Ensino e Pesquisa

andrey.silva@icen.ufpa.br

Resumo. *Quantum Machine Learning (QML) oferece vantagens no processamento de dados complexos, mas sua execução em servidores quânticos remotos levanta preocupações de privacidade. Blind Quantum Computing (BQC) busca resolver esse problema ao ocultar dados e circuitos do servidor, embora exija maior consumo de pares EPR na rede quântica. Este trabalho simula uma rede quântica federada com múltiplos clientes treinando modelos QML usando os protocolos BFK e CHILDS, avaliando o impacto na qualidade do aprendizado e no consumo de recursos.*

Abstract. *Quantum Machine Learning (QML) offers advantages in processing complex data, but executing it on remote quantum servers raises privacy concerns. Blind Quantum Computing (BQC) addresses this by hiding data and circuits from the server, although it requires higher EPR pair consumption in the quantum network. This work simulates a federated quantum network with multiple clients training QML models using the BFK and CHILDS protocols, evaluating impacts on learning quality and resource consumption.*

1. Introdução

O avanço da miniaturização de transistores impulsionado pela Lei de Moore encontra-se próximo do fim [Shalf 2020], especialmente à medida que se aproxima da escala atômica, indicando que os limites tecno-econômicos da computação clássica poderão se estabilizar por volta de 2025. A computação quântica surge como uma das alternativas mais promissoras para superar esse desafio, destacando-se por diversos motivos, entre eles as propriedades quânticas do qubit (unidade básica da informação da computação quântica) como a superposição e o emaranhamento, que permitem processar informações de maneira exponencialmente mais eficiente do que os sistemas clássicos.

A computação quântica é uma área emergente que, ao longo dos anos, tem proporcionado novas perspectivas em diferentes campos da ciência da computação, especialmente na comunicação e no aprendizado de máquina. Suas aplicações se destacam em relação à computação clássica, tanto pela maior segurança quanto pela elevada capacidade de processamento. Contudo, todas essas vantagens ainda estão distantes da realidade em termos de acessibilidade de hardware. No Brasil, por exemplo, a computação quântica ainda se encontra em estágio inicial se comparada a outros países. Dessa forma, dependemos de tecnologias desenvolvidas no exterior, o que eleva os custos e torna inviável a adoção direta.

Entretanto, nesse tipo de comunicação, é fundamental que o cliente confie no servidor, garantindo que a execução das tarefas não resulte em roubo de dados. É nesse contexto que surge a computação quântica cega (Blind Quantum Computing – BQC), cujo objetivo central é assegurar que, em uma rede quântica, o servidor execute as tarefas solicitadas pelo cliente sem, contudo, ter acesso ao conteúdo da execução. Assim, protege-se a integridade das informações e evita-se a exposição de dados sensíveis. Para alcançar esse objetivo, são utilizados protocolos específicos. Nas simulações realizadas, adotamos os protocolos BFK (Broadbent–Fitzsimons–Kashefi) e Childs, escolhidos por serem os mais consolidados na literatura e por representarem a base de diversas propostas subsequentes, além de possibilitarem uma implementação mais acessível para os estágios iniciais de experimentação.

Nesta pesquisa, abordamos também o aprendizado de máquina quântico (Quantum Machine Learning – QML), uma área que vem desempenhando um papel inovador na computação devido à sua capacidade de lidar com grandes volumes de dados, identificar padrões complexos e realizar previsões precisas, pois combina as propriedades do processamento quântico com as técnicas de aprendizado de máquina, possibilitando ganhos de desempenho significativos em tarefas como classificação, otimização e reconhecimento de padrões.

Este artigo atua como uma extensão direta e prática dessas propostas. O objetivo é simular e avaliar o desempenho de uma rede federada quântica, onde clientes compartilham pares EPR para treinar colaborativamente modelos de QML, adotando Redes Neurais Quânticas (QNN) ocultadas pelos protocolos BFK e CHILDS. Após a execução remota, os resultados são devolvidos aos clientes, o que possibilita a análise comparativa de aspectos e avaliar os *trade-offs* entre a precisão do aprendizado de máquina e o custo em recursos de rede (consumo de EPRs e fidelidade). Este estudo evidencia a relevância de uma área ainda pouco explorada, abrindo perspectivas promissoras para a continuidade do projeto e para o desenvolvimento de pesquisas futuras, que tendem a gerar contribuições significativas para a comunidade científica.

2. Fundamentação Teórica

Nesta seção, apresentam-se os fundamentos teóricos necessários para a compreensão deste trabalho, abordando os conceitos de computação quântica cega, aprendizado de máquina quântico e os conjuntos de dados utilizados.

2.1. Computação Quântica Cega (BQC) e Protocolos de Segurança

A Computação Quântica Cega (*Blind Quantum Computing* - BQC) surgiu como uma das propostas mais relevantes para viabilizar a delegação segura de tarefas computacionais em ambientes quânticos. Nesse modelo, um cliente com recursos limitados pode realizar computações complexas em um servidor quântico sem revelar suas entradas, circuito ou resultados, para garantir a proteção e a integridade das informações em redes federadas, a literatura destaca protocolos específicos:

- **Protocolo BFK (Broadbent-Fitzsimons-Kashefi):** Este protocolo baseia-se no modelo de computação quântica baseada em medições (*Measurement-Based Quantum Computing* - MBQC). O funcionamento ocorre através de um fluxo unidirecional onde o cliente, possuindo apenas um preparador de estados de um

único qubit, envia ao servidor qubits na forma $+_\theta = \frac{1}{\sqrt{2}}(0 + e^{i\theta}1)$, onde θ é um ângulo escolhido aleatoriamente pelo cliente. O servidor emaranha esses qubits em um estado de grafo (cluster state) e realiza medições sob comando do cliente. Como o servidor desconhece os ângulos θ iniciais, ele não consegue distinguir as rotações aplicadas nem o algoritmo executado, garantindo a cegueira da computação [Broadbent et al. 2009]. Por exigir apenas o envio de qubits individuais do cliente para o servidor, sua demanda por recursos de rede e fidelidade de enlace é comparativamente menor.

- **Protocolo CHILDS:** Diferente do modelo baseado em medições, o protocolo proposto por Childs (2005) utiliza um esquema de "teletransporte de portas quânticas"e opera de forma bidirecional. O cliente "esconde"seu estado quântico aplicando operadores de Pauli (X e Z) aleatórios (uma técnica de *one-time pad* quântico) antes de delegar a operação. Para que o servidor processe esses dados sem decifrá-los, o protocolo exige múltiplas interações onde qubits são enviados ao servidor, processados e retornados ao cliente para correções de fase e reenvio. Este processo é altamente dependente da distribuição de pares EPR (*Einstein-Podolsky-Rosen*) e do consumo de bits clássicos para sincronização, o que explica o elevado consumo de recursos de rede observado nas simulações deste trabalho quando comparado ao protocolo BFK [Childs 2005].

Em ambos os casos, a confidencialidade é mantida, mas cada protocolo impõe diferentes demandas de comunicação e de gerenciamento de recursos, especialmente no que tange ao consumo de pares EPR.

2.2. Quantum Machine Learning (QML) e Redes Neurais Quânticas (QNN)

O Aprendizado de Máquina Quântico (QML) busca explorar as propriedades da mecânica quântica, como superposição e emaranhamento, na construção de modelos de aprendizado. O avanço recente no QML evidencia o potencial da computação quântica para resolver problemas complexos de otimização e reconhecimento de padrões de forma mais eficiente que modelos clássicos.

- **QNN (Quantum Neural Network):** Trata-se de um modelo inspirado em redes neurais clássicas, mas que substitui as camadas tradicionais por circuitos quânticos parametrizados, empregando portas quânticas para processar informações, buscando obter vantagens sobre arquiteturas clássicas. Apesar de promissor, enfrenta desafios relacionados à escalabilidade e ao custo de treinamento (*Barren Plateaus*) em hardware quântico atual.

2.3. Conjuntos de Dados (Datasets) para Avaliação

Para mensurar o desempenho das topologias e algoritmos simulados, foram selecionados conjuntos de dados que representam diferentes níveis de complexidade:

- **Iris Dataset:** Conjunto de dados clássico composto por 150 amostras de flores com quatro atributos numéricos. É amplamente utilizado como *benchmark* para verificar a adaptação de modelos quânticos a problemas de classificação convencionais.

- **MNISQ (MNIST Quantum):** Versão adaptada do dataset MNIST de dígitos manuscritos (28×28 pixels). O MNISQ consiste em uma transformação das imagens originais para representações reduzidas (via PCA) compatíveis com circuitos quânticos, permitindo explorar a viabilidade de modelos quânticos em tarefas de visão computacional.
- **Plus-Minus:** Conjunto de dados sintético binário utilizado para validação inicial e testes de convergência do modelo sob diferentes condições de estresse de rede.

3. Metodologia

Para realizar os experimentos, foi utilizado o simulador QuantumNet, desenvolvido pelo GERCOM/UFPA. Este simulador abstrai as complexidades de hardware, facilitando a implementação de algoritmos distribuídos em redes quânticas. A topologia simulada foi configurada com 6 clientes treinando modelos colaborativamente de forma federada. Utilizamos modelos do tipo QNN com um *Batch Size* de 32 e número de amostras (*Shots*) variando entre 128 e 256. Os testes abrangeram três conjuntos de dados distintos:

- **Iris Dataset:** Conjunto clássico com 150 amostras (50 épocas).
- **MNISQ:** Versão quântica do dataset MNIST de dígitos manuscritos (5 épocas).
- **Plus-Minus:** Conjunto de dados sintético binário (20 épocas).

Para avaliar a eficiência do escalonamento de recursos, foram configurados dois perfis de agendamento de requisições:

- **Cenário 1:** Apresenta o agendamento das requisições de forma que pode-se executar protocolos em caminhos diferentes, porém no mesmo *timeslot*.
- **Cenário 2:** Apresenta o agendamento das requisições de forma que pode-se executar uma requisição de cada caminho, então a cada *timeslot* pode-se executar até quantos caminhos tiverem disponíveis.

4. Resultados e Discussão

Nesta seção, analisa-se o desempenho dos modelos de Aprendizado de Máquina Quântico (QML) federado sob diferentes protocolos de Computação Quântica Cega (BQC) e lógicas de agendamento. A Tabela 1 compila as métricas globais de convergência e infraestrutura obtidas nas simulações.

Tabela 1. Resultados: Métricas de QML e Infraestrutura de Rede.

Dataset - Configuração	Prot. BQC	Cen.	Acurácia	F1-Score	Fid. Média	EPRs (App)
1. Iris	BFK	1	0.8000	0.7885	0.8625	388
2. Iris	BFK	2	0.7556	0.7318	0.8513	30.600
3. Iris	CHILDS	1	0.8000	0.7885	0.8755	824
4. Iris	CHILDS	2	0.7556	0.7318	0.8641	61.200
5. MNISQ	CHILDS	1	0.5067	0.4831	0.8224	192
6. MNISQ	CHILDS	2	0.5067	0.4831	0.8663	1.440
7. MNISQ	BFK	1	0.5067	0.4831	0.7038	42
8. MNISQ	BFK	2	0.5067	0.4831	0.7308	720
9. Plus Minus	CHILDS	1	0.9250	0.9262	0.9572	196
10. Plus Minus	CHILDS	2	0.9250	0.9262	0.9610	5.040
11. Plus Minus	BFK	1	0.9250	0.9262	0.9357	90
12. Plus Minus	BFK	2	0.9250	0.9262	0.9352	2.520

4.1. Análise do Desempenho do QML e Fidelidade Quântica

As métricas de aprendizado (*Acurácia* e *F1-Score*) não sofrem variações extremas pela escolha do protocolo BQC, uma vez que BFK e CHILDS são matematicamente equivalentes na ocultação do dado para o servidor. Contudo, observou-se que a acurácia do modelo de QML é diretamente sensível à política de escalonamento utilizada na rede quântica.

Para o dataset Iris no Cenário 1 (agendamento de múltiplas rotas no mesmo *timeslot*), obteve-se acurácia de 80%. O dataset Plus-Minus atingiu $92,5\%$ devido à sua menor complexidade dimensional. Em contrapartida, o MNISQ registrou acurácia de $50,67\%$, refletindo os desafios intrínsecos de escalabilidade e a necessidade de redução de dimensionalidade extrema para circuitos restritos.

A transição para o Cenário 2 (agendamento por disponibilidade de caminho a cada *timeslot*) causou uma degradação notável na acurácia do Iris (caindo de 80% para $75,56\%$), esta queda demonstra que tentar despensar requisições paralelamente de forma independente por caminho gera gargalos de sincronização. Esse fenômeno prolonga a exposição dos qubits no canal clássico/quântico e reduz ligeiramente a *Fidelidade Média* das operações, afetando a precisão final na atualização dos pesos do modelo federado.

4.2. Análise do Consumo de Recursos Quânticos

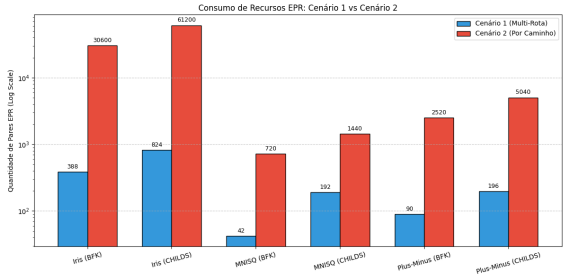

Figura 1. Comparação do consumo de pares EPR entre os Cenários 1 e 2 em escala logarítmica. O aumento exponencial no Cenário 2 reflete a ineficiência do agendamento baseado puramente em disponibilidade de caminho.

Os resultados evidenciam que o protocolo CHILDS consome consistentemente mais recursos EPR que o BFK, validando sua natureza bidirecional que exige múltiplos teletransportes de portas, independentemente da forma de escalonamento escolhida.

- **Cenário 1 (Agendamento Multi-Rota):** Esta abordagem demonstrou ser altamente econômica. Para o Iris, o BFK utilizou apenas 388 pares EPRs, enquanto o CHILDS exigiu 824 para obter o exato mesmo desempenho de acurácia.
- **Cenário 2 (Agendamento por Caminho Disponível):** Embora maximize a utilização teórica dos enlaces por *timeslot*, essa lógica de agendamento acarreta um enorme *overhead* operacional na alocação da infraestrutura. O consumo saltou exorbitantemente para 30.600 EPRs no BFK (Linha 2) e para 61.200 EPRs no CHILDS (Linha 4), um aumento de aproximadamente $75\times$ na demanda de recursos em relação ao Cenário 1.

Esses dados demonstram que, embora o CHILDS forneça uma abstração de programação mais intuitiva, o protocolo BFK é substancialmente mais eficiente. Mais importante ainda,

os resultados comprovam que adotar políticas de agendamento por caminhos independentes (Cenário 2) torna a rede quântica inviável na prática devido ao desperdício massivo de EPRs, justificando a adoção de estratégias de gerenciamento e fatiamento rigorosos.

5. Conclusão

Este trabalho demonstrou que tanto a escolha do protocolo de Computação Quântica Cega quanto a política de agendamento de recursos impactam criticamente a viabilidade de redes quânticas federadas em ecossistemas NISQ. O protocolo BFK mostrou-se a opção superior para ambientes com recursos EPR escassos, mantendo o poder de aprendizado do modelo com uma fração mínima do custo imposto pelo CHILDS.

Adicionalmente, conclui-se que lógicas de escalonamento agressivas que priorizam a execução por caminhos avulsos a cada *timeslot* (Cenário 2) geram degradação na fidelidade do aprendizado e um *overhead* insustentável na geração de EPRs. Em contrapartida, o agendamento consolidado de rotas (Cenário 1) provou ser altamente otimizado. Trabalhos futuros focarão na integração de técnicas de *network slicing* em tempo real e algoritmos adaptativos para gerenciar os *timeslots*, visando suprimir desperdícios de alocação e aumentar a resiliência do QML federado.

Em pesquisas futuras, planeja-se ampliar o escopo da avaliação para topologias complexas e explorar o gerenciamento distribuído de recursos para otimizar a latência e a escalabilidade. Objetiva-se, ainda, integrar a solução com protocolos de verificação de integridade em Computação Quântica Cega.

Agradecimentos

Este trabalho foi parcialmente financiado pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) por meio dos auxílios nº 403539/2020-0 e nº 400111/2023-3; e pela Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), sob os auxílios 2023/00811-0, 2023/00673-7, 2021/00199-8 (CPE SMARTNESS), 2020/04031-1 e 2018/23097-3. Também contou com o apoio da Propesp/UFPA, e da Venturus e da Fundação Guamá, por meio da proposta técnica 002/2025 – CITIAMAZON.

Referências

Broadbent, A., Fitzsimons, J., and Kashefi, E. (2009). Universal blind quantum computation. In *50th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 517–526. IEEE.

Childs, A. M. (2005). Secure assisted quantum computation. *Quantum Information & Computation*, 5(6):456–466.

de Abreu, D. M. and Abelém, A. J. G. (2025). Towards Blind Quantum Machine Learning in Entanglement Networks. In *Proceedings of the ACM*. ACM.

de Abreu, D. M., Moura, D. F., Rothenberg, C. E., and Abelém, A. J. G. (2025). Rede Generativa Adversarial Quântica Semi-Supervisionada (sQGAN) para Detecção de Ataques. In *Anais do XLIII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)*, pages 252–265. SBC.

Shalf, J. (2020). The future of computing beyond moore's law. *Philosophical Transactions of the Royal Society A*.