# Estudo e Simulação de uma Rede de Distribuição de Chaves Quânticas de Alto Desempenho para o Campus da UFPA

**David Tavares**[1], **Arthur Pimentel**[1], **Diego Abreu**[1], **Antônio Abelém**[1]

[1] Universidade Federal do Pará (UFPA)

david.tavares@icen.ufpa.br,arthur.pimentel@icen.ufpa.br,
diego.abreu@itec.ufpa.br,abelem@ufpa.br

***Abstract.*** *This paper presents the design and simulation of a Quantum Key Distribution (QKD) network tailored for the University Federal do Pará (UFPA) campus. By strategically placing QKD nodes, the network aims to cater to the communication needs of diverse research institutes. Simulation parameters, including inter-node distances and quantum key rates, were chosen to reflect real-world conditions. Simulation results demonstrate the viability of the proposed QKD network, showcasing its potential for high demand secure key exchange, and allowing security applications such as authentication and cryptography. This endeavor not only enhances campus communication security but also sets a precedent for implementing QKD networks in similar academic settings.*

## 1. Introdução

No cenário atual de crescentes ameaças cibernéticas e violações de segurança, a busca por mecanismos robustos e de alto desempenho para proteção de dados e comunicações tem se tornado uma prioridade tecnológica. A segurança da informação desempenha um papel vital, não somente na proteção de informações sensíveis, mas também na garantia da confiabilidade e da integridade das comunicações em diversos setores da sociedade. Nesse contexto, a Distribuição de Chaves Quânticas (*Quantum Key Distribution* - QKD) se apresenta como uma abordagem inovadora para estabelecer chaves criptográficas invioláveis, baseando-se em princípios da mecânica quântica [Abelem et al. 2023].

O protocolo de QKD, fundamentado nos princípios da mecânica quântica, possibilita a criação de chaves de criptografia compartilhadas entre duas partes, assegurando a detecção de quaisquer tentativas de interceptação não autorizada. Ao aproveitar a propriedade da indeterminação quântica, o QKD oferece uma camada adicional de segurança, fornecendo um meio para identificar e quantificar quaisquer modificações indevidas na chave compartilhada. Essa capacidade de detecção de intrusões faz do QKD uma alternativa extremamente atrativa em comparação com as técnicas de criptografia clássica, que podem ser vulneráveis a ataques computacionais avançados. No entanto, a implementação de uma rede QKD de alto desempenho apresenta desafios complexos. Primeiramente, a tecnologia quântica atual requer controle rigoroso de operação e sistemas altamente precisos, o que aumenta os custos de implementação. Além disso, a expansão de redes QKD para atender a demandas de larga escala exige soluções de hardware e software adequados. A integração eficiente do QKD em infraestruturas de comunicação existentes também é um desafio, exigindo a superação de obstáculos técnicos e logísticos.

Este artigo se propõe a apresentar um projeto de uma rede QKD customizada para atender às demandas específicas do campus da Universidade Federal do Pará (UFPA). A

UFPA, como instituição de renome em pesquisa e inovação, reconhece a importância crítica da segurança de suas comunicações. A escolha estratégica de locais para a implantação dos nós QKD, bem como a simulação abrangente da rede, são discutidas nas próximas seções. Os resultados obtidos da simulação reforçam a viabilidade e a eficácia da rede QKD proposta, demonstrando seu potencial para elevar os padrões de segurança de comunicação em um ambiente acadêmico e de pesquisa.

## 2. Rede de Distribuição de Chaves Quânticas

Os princípios essenciais da computação quântica desempenham um papel crucial na compreensão dos fundamentos do QKD. A mecânica quântica postula a superposição e a emaranhamento de estados, permitindo que sistemas quânticos existam em múltiplos estados simultaneamente [Abreu et al. 2022]. Esses princípios habilitam a criação de pares de partículas entrelaçadas que podem ser utilizados para estabelecer chaves criptográficas. A observação de uma dessas partículas influencia instantaneamente o estado da outra, criando a base para detectar qualquer tentativa de interceptação.

O funcionamento do QKD envolve a troca de informações quânticas entre duas partes, geralmente chamadas de *Alice* e *Bob*. O protocolo BB84, é o principal exemplo de QKD. Nele, Alice codifica informações em estados quânticos (como polarização de fótons), cria pares de partículas entrelaçadas e envia-os a Bob. Utilizando bases de medição compartilhadas previamente, Bob mede os fótons recebidos e comunica os resultados a Alice. A partir dessas informações, Alice e Bob podem inferir uma chave criptográfica compartilhada, detectando interferências devido a ação de agentes maliciosos.

Uma rede de distribuição de chaves quânticas é composta por uma série de nós QKD interconectados por links quânticos. Um nó QKD é formado por um módulo QKD, que lida com a função de pós-processamento das chaves quânticas, pelo Sistema de Gerenciamento de Chaves (KMS), que é responsável por funções complexas de gerenciamento, como armazenamento de chaves, sincronização e fornecimento de chaves, essenciais para redes QKD em grande escala, o Controlador de Rede QKD, responsável pelo roteamento e troca de informações da topologia e camada de aplicação (APP), responsável pela aplicação de autenticação ou criptografia [Mehic et al. 2017]. A troca segura de chaves ocorre entre esses nós, garantindo comunicações protegidas entre pontos remotos. Além da segurança de comunicações, redes QKD têm potencial para aplicações como a distribuição de chaves para sistemas de criptografia clássica, a autenticação quântica e a criação de redes de sensores quânticos. A estrutura da rede pode variar, desde topologias simples com nós interconectados até configurações mais complexas que abrangem distâncias maiores.

## 3. Metodologia e Experimentos

Para o projeto da rede QKD, escolheu-se utilizar o simulador OpenQKD[1]. Este simulador tem sido utilizado no projeto de mais 32 ambientes de experimentação de QKD na Europa, abrangendo desde redes de campus e metropolitanas até redes nacionais, com links superiores a 100km. Além disso, o OpenQDK foi projetado com base nas normas ETSI 0004 e ETSI 0014 [ETS ], que padronizam o funcionamento de redes QKD e dão suporte

[1]https://openqkd.eu/


**Figura 1. Rede QKD proposta para o Campus da UFPA no simulador OpenQKD**

a diversos dispositivos QKD disponíveis no mercado. Assim, é o sistema ideal para servir como base para o projeto da rede QDK proposto.

Para a simulação da rede QKD da UFPA, definiram-se 4 locais para alocação dos nós quânticos, sendo eles: CTIC (Centro de Tecnologia da Informação e Comunicação) - Nó 1, LABITC (Laboratório de Tecnologias de Informação e Comunicação) - Nó 2, ITEC (Instituto de Tecnologia) - Nó 3, e Hospital Universitário Betina - Nó 4. Dessa forma, a rede poderá abranger tanto o campo profissional, básico e de saúde da UFPA, onde se encontram diversos centros de pesquisa e pontos de interesse da comunidade acadêmica. A Figura 1 mostra a configuração escolhida.

A Tabela 1 detalha as especificações do experimento. A rede tem uma topologia em linha, composta por 4 links. Cada link tem uma distância específica e uma taxa de geração de chaves (*KeyRate*), determinada pelo simulador baseando-se na distância, e tamanho da chave (*KeySize*) configurada para 10kb. Em cada link, implementou-se uma aplicação de autenticação e criptografia que usa as chaves distribuídas. O simulador disponibiliza técnicas de autenticação e de criptografia, que foram empregadas na simulação: VMAC (*Message Authentication Code using Universal Hashing*) para autenticação e OTP (*One-time pad*) para criptografia. Adicionalmente, a taxa de uso da aplicação (AppRate) foi estabelecida em 20Kb/s, mantendo a configuração padrão.

**Tabela 1. Configurações do Experimento.**

| **QKD link** | Distância | KeyRate Calculada | KeySize | AppRate |
|---|---|---|---|---|
| Link 1-2 | 591 (m) | 1463 (kbps) | 10 kb | 20Kb/s |
| Link 2-3 | 498 (m) | 1736 (kbps) | 10 kb | 20Kb/s |
| Link 3-4 | 945 (m) | 915 (kbps) | 10kb | 20Kb/s |

A Figura 1 apresenta o funcionamento da rede em termos de pares de chaves QKD geradas pelo KMS e pares de chaves consumidas pelas aplicações, quando utilizado o valor de *keyrate* recomendado pelo simulador. Se considerarmos o valor de *keyrate* mínimo (5kbps), teremos menos chaves geradas do que o necessário para aplicação, isso pode ser observado na Figura 2. Como consequência, a taxa de chaves corretamente geradas diminui (KDU - *Key data utilization*) e o número de notificações de pacotes perdidos (MC - *Missed Calls*) aumenta. Na Tabela 2 é possível ver de forma detalhada a relação entre o key rate, KDU e MC, em dois experimentos. No primeiro é utilizado apenas uma

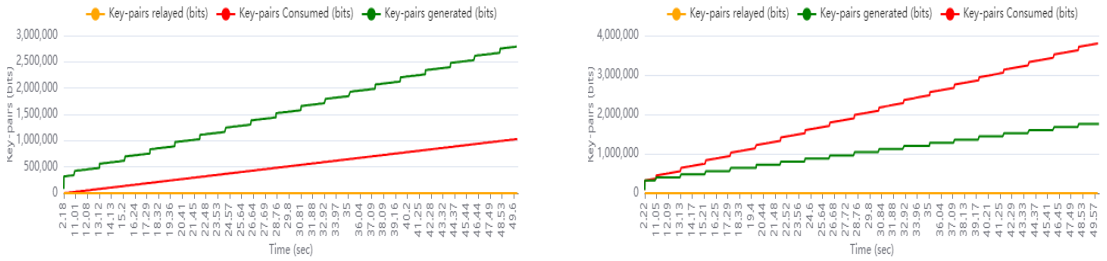


**Figura 2. Consumo e Geração de Chaves com o *key rate*: (a) no valor recomendado e (b) no valor mínimo de 5kbps.**

aplicação de autenticação ou de criptografia, ambas resultam nos mesmo valores de KDU e MC. No segundo, são implementadas ambas aplicações em todos os links. Para ambos os experimentos, a autenticação utilizada foi o VMAC e a criptografia foi o OTP.

**Tabela 2. Resultados dos Experimento para rede QKD UFPA.**

| **Aplicação** | KeyRate | 5kbps | 10kbps | 15kbps | 20kbps | 100kbps | 500kbps |
|---|---|---|---|---|---|---|---|
| VMAC ou OTP | KDU | 23.30% | 69.80% | 69.80% | 77.30% | 98.80% | 98.80% |
| | MC | 767 | 302 | 302 | 227 | 2 | 2 |
| VMAC + OTP | KDU | 11.61% | 35.10% | 47.30% | 69.80% | 98.80% | 98.80% |
| | MC | 884 | 649 | 527 | 302 | 2 | 2 |

## 4. Conclusão e Trabalhos Futuros

Neste trabalho foi realizado o estudo e simulação de uma rede QKD para o campus da UFPA. Os resultados da simulação demonstram que a rede é viável, fornecendo taxas de geração de chaves satisfatórias para aplicações de autenticação e criptografia em diferentes pontos do campus. Como trabalhos futuros, propomos explorar outras topologias de rede, otimizar os parâmetros de simulação para atender a requisitos específicos de segurança e desempenho e expandir a rede para atender a demandas adicionais. Além disso, a pesquisa em algoritmos de criptografia quântica e técnicas de autenticação quântica pode aprimorar ainda mais a segurança das comunicações na rede QKD da UFPA. Em última análise, esse projeto serve como um ponto de partida para futuras iniciativas em redes metropolitanas como a Metrobel e nacionais como a RNP (Rede Nacional de Ensino e Pesquisa).

## Referências

ETSI 2022. Quantum Key Distribution (QKD). `https://www.etsi.org/committee/1430-qkd`. Accesso em 02 de Setembro de 2023.

Abelem, A., Towsley, D., and Vardoyan, G. (2023). Quantum internet: The future of internetworking. *arXiv preprint arXiv:2305.00598*.

Abreu, D., Abelém, A., and Rothenberg, C. (2022). Desafios e oportunidades de pesquisa para o roteamento em redes quânticas. In *Anais do II Workshop de Comunicação e Computação Quântica*, pages 37–42, Porto Alegre, RS, Brasil. SBC.

Mehic, M., Maurhart, O., Rass, S., and Voznak, M. (2017). Implementation of quantum key distribution network simulation module in the network simulator ns-3. *Quantum Information Processing*, 16:1–23.