Uma Abordagem para Prototipagem de Aplicações com Distribuição Quântica de Chaves

Anderson Tomkelski[1], Marcus Freire[1,2], Maycon Peixoto[2], João Souza[1], Valéria Silva[1], Ricardo Parizotto[1]

[1]QuIIN – Quantum Industrial Innovation,
Centro de Competência EMBRAPII CIMATEC em Tecnologias Quânticas,
SENAI CIMATEC, Av. Orlando Gomes 1845, 41650-010, Salvador, BA, Brasil.

{anderson.tomkelski,joao.marcelo,valeria.dasilva,ricardo.parizotto}fbter.org.br

[2]Instituto de Computação, Universidade Federal da Bahia (UFBA)
Avenida Milton Santos, s/n, PAF 2, 40.170-110 – Salvador – Bahia – Brasil

{marcus.elias,maycon.leone}@ufba.br

Abstract. *Quantum Key Distribution (QKD) is a cryptographic technique based on the principles of quantum mechanics, aimed at securely establishing secret keys between parties. Despite significant advances in the field, there are still major challenges to its practical adoption, particularly in applications such as virtual private networks and end-to-end security. In this work, we propose an approach to prototype QKD-based applications by combining co-simulation techniques that integrate quantum simulators with network emulators. This integration enables prototyping in a flexible environment without requiring modifications to support a real QKD network. As a proof of concept, we implemented a private network application and evaluated its functionality.*

Resumo. *A Distribuição Quântica de Chaves (QKD) é uma técnica criptográfica baseada nos princípios da mecânica quântica, voltada para o estabelecimento seguro de chaves secretas entre partes. Apesar dos avanços na área, ainda existem lacunas importantes para sua adoção prática, especialmente em aplicações como redes privadas virtuais e segurança ponto a ponto. Neste trabalho, propomos uma abordagem para prototipagem de aplicações que utilizam QKD, combinando técnicas de co-simulação entre simuladores quânticos e emuladores de rede. Essa integração permite desenvolver protótipos em um ambiente flexível, sem a necessidade de modificações específicas para suportar uma rede QKD real. Como prova de conceito, implementamos uma aplicação de rede privada e avaliamos sua funcionalidade.*

1. Introdução

Os mecanismos criptográficos clássicos, baseados em problemas matemáticos complexos, estão cada vez mais vulneráveis diante do avanço das capacidades computacionais — em especial com o surgimento da computação quântica. Algoritmos quânticos, como o de Shor, representam uma ameaça concreta aos sistemas de chave pública amplamente utilizados atualmente. Nesse cenário, surgem duas abordagens principais para a segurança no mundo pós-quântico: a criptografia pós-quântica (PQC), ainda baseada em matemática

clássica, e a criptografia quântica, fundamentada nas leis da física quântica. Entre estas, a Distribuição Quântica de Chaves (Quantum Key Distribution - QKD) destaca-se como uma tecnologia promissora, oferecendo segurança informacionalmente teórica para o estabelecimento de chaves secretas entre partes remotas [Dervisevic et al. 2025].

Diferente dos métodos tradicionais de troca de chaves, a QKD utiliza canais quânticos para transmissão de bits e canais públicos autenticados para verificação, o que garante que qualquer tentativa de interceptação possa ser detectada. Apesar de enfrentar desafios como a necessidade de infraestrutura física dedicada e restrições de escalabilidade, a incorruptibilidade dos princípios físicos que fundamentam a QKD a posiciona como uma das alternativas mais promissoras para o futuro da segurança de redes.

Apesar dos avanços obtidos com o uso de QKD, existem importantes lacunas ainda não completamente solucionadas. Em particular, destacam-se desafios relacionados à integração efetiva entre infraestruturas quânticas e redes clássicas, bem como questões de interoperabilidade entre dispositivos e protocolos heterogêneos [Mehic et al. 2020]. Além disso, o alto custo dos equipamentos QKD representa uma barreira significativa, impactando não apenas os custos envolvidos no desenvolvimento de novas aplicações, mas também a própria viabilidade de implantação. Devido a esse custo elevado, a quantidade de dispositivos disponíveis costuma ser limitada, o que dificulta a realização de testes isolados sem afetar aplicações já em funcionamento.

Neste trabalho, propomos uma abordagem para prototipação de aplicações que integram redes clássicas e dispositivos de distribuição quântica de chaves. A proposta utiliza uma plataforma de co-simulação que combina o simulador quântico NetSquid, responsável por gerar chaves seguras através do protocolo QKD (por exemplo, o BB84), com emuladores de redes definidas por software, como Mininet e BMv2. Nossa solução envolve ainda um serviço de gerenciamento de chaves (KMS), que facilita o armazenamento, a distribuição e o uso das chaves geradas pelo processo QKD. Para mostrar um caso de uso funcional, utilizaremos o protocolo IPsec integrado ao KMS, permitindo que as chaves sejam utilizadas para conectar hosts de uma rede clássica emulada. As principais contribuições deste trabalho incluem: **(i)** Metodologia para validação experimental de interoperabilidade entre redes clássicas e quânticas. **(ii)**Definição e implementação de um gateway que atua como intermediário entre os domínios quântico e clássico. **(iii)** Demonstração prática de comunicação segura baseada em protocolos criptográficos padrão como o IPsec.

2. Contextualização e Trabalhos Relacionados

QKD é uma técnica criptográfica baseada nos princípios da mecânica quântica, em especial no princípio da incerteza de Heisenberg e na não clonagem de estados quânticos. A principal vantagem da QKD reside no fato de que qualquer tentativa de interceptação altera o estado quântico da informação, permitindo sua detecção. O protocolo BB84, proposto por Bennett e Brassard em 1984, é o primeiro e mais conhecido protocolo de QKD. Nele, o emissor (Alice) envia fótons polarizados em bases aleatórias (retas ou diagonais), codificando bits. O receptor (Bob), por sua vez, mede esses fótons também em bases escolhidas aleatoriamente. Após a transmissão, ambos comparam publicamente as bases utilizadas e descartam os bits em que houve discordância, resultando em uma chave secreta compartilhada — cuja segurança é garantida pela própria física quântica

Autor / Ano	Objetivo principal	Integração redes clássicas?	QKD	PQC	KMS	Simulação/Emulação
[Mehic et al. 2020]	Panorama de redes QKD (topologias, roteamento, SDN)	✓ — integração IPsec/VPN e SDN	✓	✗	✓	✗ — não informado
[James et al. 2023]	Arquitetura KMS para QKD, APIs KMS-to-KMS / SDN	✓ — REST/CoAP + SDN	✓	✓	✓	✗ — não informado
[Garcia et al. 2024]	Implementar e avaliar TLS híbrido PQC + QKD (concatenação e XOR) medindo desempenho e segurança	✓ — TLS 1.2 modificado sobre IP; chaves QKD via API ETSI	✓	✓	✓	✗ — testbed físico
[Dervisevic et al. 2025]	Revisão e comparação de KMS em redes QKD	✓ — hop-by-hop (VPN/IPsec)	✓	✗	✓	✗ — não informado
[Buruaga et al. 2025]	TLS 1.3 híbrido (DHKE + QKD + PQC) em SDN	✓ — LKMS/KPS via IP-SDN	✓	✓	✓	✗ — testbed físico
[Garcia et al. 2025]	Protocolos TLS/IPsec triplo-híbridos (clássico + PQC + QKD)	✓ — QKD via KMS REST	✓	✓	✓	✗ — testbed físico
[Gao et al. 2025]	Integrar QKD ao IPSec e propor atualização dinâmica de chaves com janela deslizante	✓ — mantém IPSec padrão; QKD via QKI sobre IP	✓	✗	✓	✗ — testbed físico
Nosso trabalho	Prototipar aplicações QKD integradas a redes clássicas via co-simulação NetSquid + Mininet e demonstrar comunicação IPsec segura	✓ — gateway HTTPS + REST ETSI entre Mininet e NetSquid	✓	✓	✓	✓ — NetSquid + Mininet/BMv2

Tabela 1. Trabalhos relacionados em segurança de redes com QKD e/ou PQC.

[Bennett and Brassard 2014].

Há trabalhos que ja apresentam integração de alguns protocolos clássicos de rede com QKD. São exemplos a integração de protocolos como IPsec [Gao et al. 2025], que protegem a camada de rede e permitem criar redes virtuais ou MACSec [Alia et al. 2025], que protegem a camada de enlace. Porém, existem poucas ferramentas que proveem meios para prototipar e testar tais integrações. As ferramentas existentes tem foco específico na troca de chaves usando canais quânticos e proveem poucos recursos para realizar a integração com uma aplicação de rede segura.

Por outro lado, a prototipação de redes de computadores pode se dar de diversas maneiras. Esforços notáveis, como no desenvolvimento do Mininet [Lantz et al. 2010], permitem a prototipação de redes em um ambiente de emulação. Tal emulação, permite, por exemplo, criar aplicações de camadas de rede, enlace e transporte, que são camadas que o QKD pode atuar. Além disso, esforços para expandir o Mininet para outros domínios, como o de Wi-FI, tem tido sucesso [Fontes et al. 2015]. Porém, ainda não há integração com o QKD.

A tabela 1 sintetiza o estado da arte em soluções que combinam Distribuição Quântica de Chaves (QKD) e criptografia pós-quântica (PQC) com mecanismos clássicos de segurança. Ao emular simultaneamente o domínio quântico e o ambiente IP convencional, tais testbeds permitem validar desempenho, interoperabilidade e escalabilidade com baixo custo, acelerando a transição rumo às infraestruturas de comunicação seguras exigidas no cenário pós-quântico.

3. Design

Nesta seção, nós apresentamos a visão geral de nossa abordagem para prototipar aplicações que combinam redes clássicas com QKD. A abordagem permite desenvolver

e testar aplicações de QKD e testar em um ambiente emulado, integrando métricas tanto relacionadas a distribuição de chaves, mas também de comunicação clássica.

3.1. Visão geral

A Figura 1 apresenta uma visão geral da abordagem proposta para suportar a prototipação de aplicações integradas ao QKD.

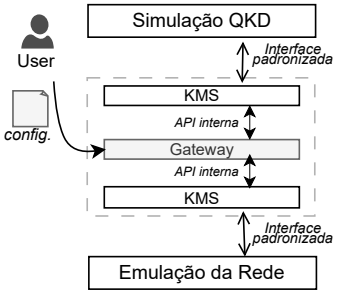

Figura 1. Arquitetura geral da abordagem de prototipação.

A visão de alto nível da abordagem proposta é composta por cinco componentes principais: o simulador de QKD, um emulador de redes programáveis e um gateway capaz de intermediar a comunicação entre eles. Além disso, um key management system (KMS) é integrado em cada dispositivo para gerenciar as chaves e requisições de chave. Por fim, um módulo de configuração permite ao usuário configurar topologias de rede, associando os dispositivos QKD aos dispositivos da rede clássica.

3.2. Workflow da Integração QKD–Rede Clássica com KMS

O processo de distribuição de chaves criptográficas na arquitetura proposta ocorre através da integração entre um ambiente de simulação quântica e uma rede clássica virtualizada. A seguir, vamos descrever o workflow da Figura 2 passo a passo.

O processo se inicia quando um host da rede clássica, como o *host 0* no ambiente Mininet, deseja iniciar uma comunicação segura. Para isso, ele utiliza uma instância local de um KMS, que fornece interface para a aplicação segura utilizar as chaves. Essa requisição é enviada para uma instância do gateway local, que checa o mapeamento de nodos em uma tabela de busca (Passo ❶) e envia uma requisição via *API REST*, e valida a requisição de acordo com o padrão *ETSI GS QKD 014*. O Gateway HTTPS funciona como a interface de comunicação entre a rede clássica e o sistema QKD. Seu papel é receber, validar e traduzir as requisições de chave da rede clássica (Mininet) em chamadas internas para o KMS apropriado do QKD. Ao fazer isso, ele abstrai a complexidade da geração e gerenciamento das chaves, além de atuar como um "roteador" para as solicitações (Passo ❷).

O KMS destino processa a requisição e busca no seu buffer interno a chave correspondente (Passo ❸). Essas chaves foram previamente geradas por meio do protocolo *BB84*, simulado no *NetSquid*, representando a comunicação entre os nós quânticos *Alice* e *Bob*. No NetSquid nós simulamos canais quânticos e canais clássicos autenticados. As chaves geradas são armazenadas em buffers na instância do KMS, permitindo a separação entre geração e consumo das chaves. Após o KMS localizar a chave em seu buffer, ele a

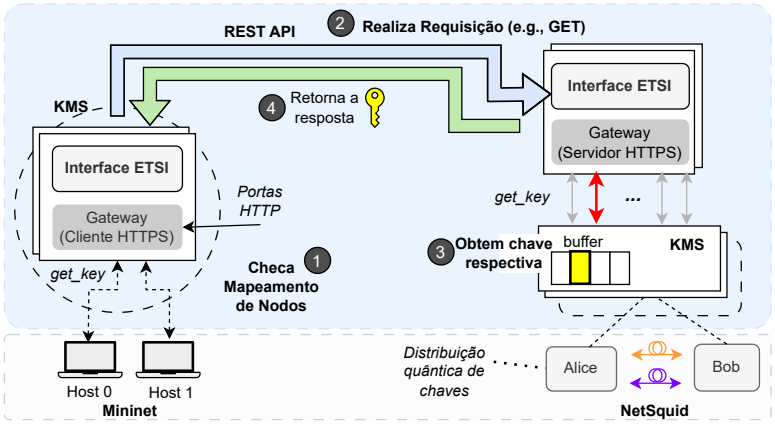

Figura 2. Fluxo de integração entre rede clássica e rede quântica com distribuição de chaves via protocolo BB84. O *Host 0*, em ambiente Mininet, realiza uma requisição de chave por meio de uma API REST padronizada (ETSI GS QKD 014), intermediada por um Gateway HTTPS. A solicitação é encaminhada ao KMS, que recupera uma chave previamente gerada entre os nós quânticos *Alice* e *Bob*, simulados no NetSquid. A chave é então retornada ao host para uso em comunicações seguras com IPsec. A arquitetura emprega buffers para desacoplar o ritmo de geração quântica e consumo clássico.

retorna para o Gateway. O Gateway então se encarrega de formatar a resposta de acordo com o padrão ETSI e encaminhá-la de volta ao host solicitante original na rede clássica, completando o fluxo da requisição (Passo ❹). Essa chave é então utilizada pelo host para realizar a comunicação segura com outro host, como o *host 1*.

4. Implementação & Caso de Uso

Para simular o QKD nós utilizamos uma implementação do protocolo BB84 no NetSquid [Coopmans et al. 2021]. A comunicação realizada através do gateway é implementada em uma API Rest em python, baseada nos padrões da ETSI. O gateway é escrito em python e utiliza um ambiente multithread para isolar a comunicação entre os nodos do mininet para os nodos QKD simulados com o NetSquid. O caso de uso é construido uilizando python e scapy para prototipar os cabeçalhos de pacotes trocados na rede do mininet. Utilizamos a configuração de uma rede virtual para encriptar a informação entre diferentes hosts, utilizando a chave obtida pelo QKD.

A seguir, descrevemos um caso de uso funcional com a nossa abordagem. Utilizamos dois hosts (Alice e Bob) implementando uma aplicação de comunicação segura. A aplicação segura ocorre em uma rede emulada no mininet, fazendo transferência de informações entre os dois hosts. A troca de mensagens acontece dentro de um grupo seguro utilizando uma rede virtual com as chaves gerados via QKD e distribuídas via KMS.

Nós apresentamos a captura de um dos pacotes gerados na Figura 3. Observamos que o *payload* do protocolo `IPv4` é corretamente encapsulado em um cabeçalho chamado *Encapsulating Security Payload*. Esse cabelçalho é direcionado pelo campo *Protocol* do `IPv4`, permitindo a realização correta do *deparsing* para o nodo que recebe o pacote.

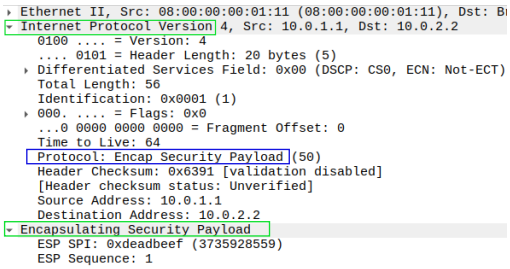

Figura 3. Demonstração do cabeçalho encapsulado pelo IpSec.

5. Discussões

Embora a abordagem apresentada já fornece flexibilidade e modularidade ao projetar novas aplicações com QKD, há ainda limitações.

Sincronização. O tempo de simulação do QKD não é diretamente compatível ao do BMv2, podendo gerar imprecisões nos resultados. Como exemplo, o tempo de geração de chaves obtido no simulador não impacta no tempo de GET de uma nova chave. Isso faz com que o impacto de taxa de geração de chaves não influencie fidedignamente as aplicações executando no Mininet. Sincronizar corretamente os dois ambientes será necessário para que as aplicações testadas enfrentem situações mais realísticas.

Topologias Maiores. Outra limitação está na configuração do gateway e do simulador do QKD, que ainda está limitado a comunicação ponto a ponto do QKD. Permitir configurar nodos confiáveis irá habilitar comunicação testes de aplicações mais robustas. Além disso, explorar um gerenciador de chaves mais robusto, com técnicas de redes definidas por software para melhorar a qualidade da troca de chaves está em perspectiva.

6. Conclusões

Existem lacunas significativas na pesquisa relacionada à integração de QKD em aplicações práticas em redes tradicionais. Em especial, destacamos a necessidade de ambientes de prototipação e teste que não gerem sobrecarga em ambientes reais. Neste trabalho, apresentamos uma abordagem de prototipação baseada em co-simulação. Integramos o BMv2 com suporte a P4 ao NetSquid e demonstramos um caso de uso utilizando o IPSec. No futuro, planejamos integrar outros protocolos, tanto em nível de hosts (i.e., TLS) quanto em nível de switches (i.e., MACsec). Além disso, pretendemos explorar técnicas mais avançadas para KMS, como redes definidas por software. Por fim, planejamos migrar as aplicações prototipadas para um ambiente com hardware real, realizando otimizações conforme as demandas específicas de cada aplicação.

7. Agradecimentos

Este trabalho foi parcialmente financiado pelo projeto QuIIN Integração CV-QKD com Redes Clássicas apoiado pelo QuIIN - Inovação Industrial Quântica, Centro de Competência EMBRAPII CIMATEC em Tecnologias Quânticas, com recursos financeiros do PPI IoT/Manufatura 4.0 do edital MCTI número 053/2023, firmado com a EMBRAPII. Este estudo também contou com financiamento, 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

[Alia et al. 2025] Alia, O., Huang, A., Lai, R., Luo, H., Goh, J., Pistoia, M., and Lim, C. (2025). Quantum-safe macsec connectivity to public cloud providers in a metropolitan network over deployed fiber. In *Optical Fiber Communication Conference*, pages Tu2D–1. Optica Publishing Group.

[Bennett and Brassard 2014] Bennett, C. H. and Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7–11. Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.

[Buruaga et al. 2025] Buruaga, J. S., Méndez, R. B., Brito, J. P., and Martin, V. (2025). Hybrid quantum-safe integration of tls in sdn networks. *Computer Networks*, page 111355.

[Coopmans et al. 2021] Coopmans, T., Knegjens, R., Dahlberg, A., Maier, D., Nijsten, L., de Oliveira Filho, J., Papendrecht, M., Rabbie, J., Rozpedek, F., Skrzypczyk, M., et al. (2021). Netsquid, a network simulator for quantum information using discrete events. *Communications Physics*, 4(1):164.

[Dervisevic et al. 2025] Dervisevic, E., Tankovic, A., Fazel, E., Kompella, R., Fazio, P., Voznak, M., and Mehic, M. (2025). Quantum key distribution networks-key management: A survey. *ACM Computing Surveys*, 57(10):1–36.

[Fontes et al. 2015] Fontes, R. R., Afzal, S., Brito, S. H., Santos, M. A., and Rothenberg, C. E. (2015). Mininet-wifi: Emulating software-defined wireless networks. In *2015 11th International conference on network and service management (CNSM)*, pages 384–389. IEEE.

[Gao et al. 2025] Gao, X., Xue, K., Li, J., Li, Z., Wu, J., Yu, N., Sun, Q., and Lu, J. (2025). Ipseq: A security-enhanced ipsec protocol integrated with quantum key distribution. *IEEE Communications Magazine*, pages 1–8.

[Garcia et al. 2025] Garcia, C. R., Aguilera, A. C., Stan, C., Vegas, J. J., Rommel, S., and Monroy, I. T. (2025). Enhanced network security protocols for the quantum era: Combining classical and post-quantum cryptography, and quantum key distribution. *IEEE Journal on Selected Areas in Communications*.

[Garcia et al. 2024] Garcia, C. R., Rommel, S., Takarabt, S., Olmos, J. J. V., Guilley, S., Nguyen, P., and Monroy, I. T. (2024). Quantum-resistant transport layer security. *Computer Communications*, 213:345–358.

[James et al. 2023] James, P., Laschet, S., Ramacher, S., and Torresetti, L. (2023). Key management systems for large-scale quantum key distribution networks. In *Proceedings of the 18th International Conference on Availability, Reliability and Security*, pages 1–9.

[Lantz et al. 2010] Lantz, B., Heller, B., and McKeown, N. (2010). A network in a laptop: rapid prototyping for software-defined networks. In *Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks*, pages 1–6.

[Mehic et al. 2020] Mehic, M., Niemiec, M., Rass, S., Ma, J., Peev, M., Aguado, A., Martin, V., Schauer, S., Poppe, A., Pacher, C., et al. (2020). Quantum key distribution: a networking perspective. *ACM Computing Surveys (CSUR)*, 53(5):1–41.