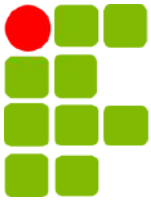


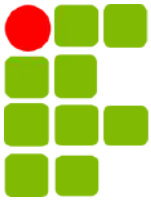
Instituto Federal de Educação, Ciência e Tecnologia da Paraíba
Campus Campina Grande
Coordenação do Curso Superior de Tecnologia em Telemática

# CRIPTOGRAFIA QUÂNTICA EM REDES 5G

MIKAEL MARINHO OLIVEIRA

Orientador: Dr. MARCELO PORTELA SOUSA

Campina Grande, 2025



Instituto Federal de Educação, Ciência e Tecnologia da Paraíba
Campus Campina Grande
Coordenação do Cursos Superior de Tecnologia em Telemática

# CRIPTOGRAFIA QUÂNTICA EM REDES 5G

MIKAEL MARINHO OLIVEIRA

Monografia apresentada à Coordenação do Curso de Telemática do IFPB - Campus Campina Grande, como requisito parcial para conclusão do curso de Tecnologia em Telemática.

Orientador: Dr. Marcelo Portela Sousa

Campina Grande, 2025

Catalogação na fonte:
Ficha catalográfica elaborada por Gustavo César Nogueira da Costa - CRB 15/479

O48c Oliveira, Mikael Marinho

Criptografia quântica em redes 5G / Mikael Marinho Oliveira. – 2025.
68 f.: il.

Trabalho de Conclusão de Curso (Graduação em Tecnologia em Telemática) - Instituto Federal da Paraíba, 2025.
Orientador: Prof. Dr. Marcelo Portela Sousa.

1.Redes 5G. 2. Criptografia quântica. 3. Distribuição de chaves quânticas (QKD). 4. Segurança da informação. I. Sousa, Marcelo Portela. II. Título.

CDU 004.738

# CRIPTOGRAFIA QUÂNTICA EM REDES 5G

**MIKAEL MARINHO OLIVEIRA**

---

Dr. Marcelo Portela Sousa
Orientador

---

Dr. Bruno de Brito Leite
Membro da Banca

---

Dr. Elmano Ramalho Cavalcante
Membro da Banca

Campina Grande, Paraíba, Brasil

Dedico este trabalho aos meus pais, que são meu maior exemplo de amor e dedicação. Nos momentos em que pensei em desistir, foram eles que mantiveram viva a chama da esperança e me incentivaram a seguir em frente.

Também dedico aos professores, que confiaram em mim mesmo quando eu duvidava de mim, e aos amigos que estiveram ao meu lado em cada passo, oferecendo apoio nos momentos mais difíceis.

Believe in yourself and all that you are. Know that there is something inside you that is greater than any obstacle

Christian D. Larson

# Agradecimentos

Agradeço primeiramente à minha família por me dar a oportunidade de concluir essa jornada, por sempre me apoiarem, me motivarem e nunca permitirem que eu desistisse; suas palavras de incentivo foram fonte de inspiração e amor em toda a minha trajetória acadêmica. Aos meus amigos, que estiveram ao meu lado nos momentos mais desafiadores, minha profunda gratidão. Aos professores Marcelo Portela, Moacy Pereira, Iana Daya, Daniela Dias, Bruno Brito, David Candeia e Ewerton Rômulo, que me apoiaram e me guiaram com dedicação, contribuindo não apenas para a conclusão do curso, mas para minha formação como profissional e ser humano com valores e princípios. Um agradecimento especial ao professor Marcelo Portela, sempre atencioso e cuidadoso com todos, um verdadeiro pai, e meu orientador, cuja orientação e apoio foram fundamentais nos momentos difíceis. Agradeço também aos colegas que estiveram comigo ao longo da jornada: Lucas, Ednaldo, Rafael, Adrian, Weslley, Galvão, Jefferson, Wesley, Giovana, Mikaio, Eduardo, Rodrigues, Jéssica, Allan, Artur, Rubens e tantos outros que fizeram parte dessa caminhada. Por fim, deixo meu sincero agradecimento ao Instituto Federal da Paraíba – Campus Campina Grande, por todo o apoio durante esses anos, fundamentais para minha formação e superação dos desafios vividos. Sem cada um de vocês, eu não teria chegado até aqui.

# Resumo

Este trabalho analisa o artigo *Quantum Cryptography in 5G Networks: A Comprehensive Overview*, destacando o uso da Distribuição de Chaves Quânticas (*Quantum Key Distribution* - QKD) como um mecanismo promissor de segurança para redes 5G. O crescimento acelerado do 5G, caracterizado por altas taxas de dados, baixa latência e grande densidade de dispositivos, impõe novos desafios de segurança que soluções tradicionais, como IPsec e MACsec, não conseguem atender plenamente sem impactar o desempenho. A QKD surge como uma alternativa capaz de fornecer segurança baseada em princípios físicos, sendo especialmente adequada para segmentos ópticos estáticos, como enlaces *fronthaul*. O estudo discute implementações práticas, limitações relacionadas à distância e interferências, bem como a necessidade de criptografadores dedicados, com baixa latência e suporte à renovação frequente de chaves. Como trabalho futuro, pretende-se aprofundar os estudos em QKD e analisar a aplicação da Criptografia Pós-Quântica (*Post-Quantum Cryptography* - PQC), buscando uma abordagem combinada que fortaleça a segurança das redes móveis de próxima geração.

**Palavras-chave:** Distribuição Quântica de Chaves (QKD); Redes 5G; Segurança de Redes; *Fronthaul*; Criptografia Pós-Quântica (PQC).

# Abstract

This work analyzes the article Quantum Cryptography in 5G Networks: A Comprehensive Overview, highlighting the use of Quantum Key Distribution (QKD) as a promising security mechanism for 5G networks. The rapid growth of 5G characterized by high data rates, low latency, and dense deployments introduces new security challenges. Traditional solutions such as IPsec and MACsec cannot fully address these issues without compromising performance. QKD emerges as a method capable of providing information-theoretic security based on the principles of quantum mechanics. It is particularly suitable for static optical segments, such as fronthaul links. This study discusses practical implementations of QKD, as well as its limitations related to distance and interference. The analysis also emphasizes the need for dedicated encryptors capable of low-latency operation and frequent key refreshing. Future work will focus on deepening the study of QKD and exploring its integration with Post-Quantum Cryptography (PQC). This combined approach aims to enhance the security of next-generation mobile networks by leveraging the strengths of both technologies.

**Keywords:** Quantum Key Distribution (QKD); 5G Networks; Network Security; Fronthaul; Post-Quantum Cryptography (PQC).

# Sumário

# Lista de Abreviaturas

| **Sigla** | **Significado** |
|---|---|
| IoT | *Internet of Things* (Internet das Coisas) |
| IIoT | *Industrial Internet of Things* (Internet Industrial das Coisas) |
| 5G | *Fifth Generation* (Quinta Geração de Redes Móveis) |
| QKD | *Quantum Key Distribution* (Distribuição Quântica de Chaves) |
| PQC | *Post-Quantum Cryptography* (Criptografia Pós-Quântica) |
| IPsec | *Internet Protocol Security* (Segurança do Protocolo de Internet) |
| MACsec | *Media Access Control Security* (Segurança de Controle de Acesso à Mídia) |
| KMS | *Key Management System* (Sistema de Gerenciamento de Chaves) |
| SKR | *Secure Key Rate* (Taxa de Chave Segura) |
| SDN | *Software-Defined Networking* (Rede Definida por Software) |
| NFV | *Network Function Virtualization* (Virtualização de Funções de Rede) |
| FPGA | *Field-Programmable Gate Array* (Matriz de Portas Programáveis em Campo) |
| PON | *Passive Optical Network* (Rede Óptica Passiva) |
| WDM | *Wavelength Division Multiplexing* (Multiplexação por Divisão de Comprimento de Onda) |
| TDM | *Time Division Multiplexing* (Multiplexação por Divisão de Tempo) |
| OTP | *One-Time Pad* (Cifra de Uso Único) |
| CO | *Central Office* (Escritório Central) |
| RAN | *Radio Access Network* (Rede de Acesso por Rádio) |
| 5GC | *5G Core* (Núcleo da Rede 5G) |
| eMBB | *Enhanced Mobile Broadband* (Banda Larga Móvel Aprimorada) |

| **Sigla** | **Significado** |
|---|---|
| URLLC | *Ultra-Reliable Low Latency Communications* (Comunicações de Baixa Latência Ultrarconfiáveis) |
| mMTC | *Massive Machine-Type Communications* (Comunicações Massivas do Tipo Máquina) |
| UE | *User Equipment* (Equipamento do Usuário) |
| RF | *Radio Frequency* (Radiofrequência) |
| C-RAN | *Cloud Radio Access Network* (Rede de Acesso por Rádio em Nuvem) |
| DU | *Distributed Unit* (Unidade Distribuída) |
| BBU | *Baseband Unit* (Unidade de Banda Base) |
| RRH | *Remote Radio Head* (Cabeça de Rádio Remota) |
| RRU | *Remote Radio Unit* (Unidade de Rádio Remota) |
| RU | *Radio Unit* (Unidade de Rádio) |
| HARQ | *Hybrid Automatic Repeat Request* (Solicitação de Repetição Automática Híbrida) |
| CU | *Centralized Unit* (Unidade Centralizada) |
| eCPRI | *Enhanced Common Public Radio Interface* (Interface de Rádio Pública Comum Aprimorada) |
| BS | *Base Station* (Estação Base) |
| MitM | *Man-in-the-Middle* (Ataque do tipo Homem-no-Meio) |
| DoS | *Denial of Service* (Negação de Serviço) |
| AKA | *Authentication and Key Agreement* (Autenticação e Acordo de Chave) |
| TCP | *Transmission Control Protocol* (Protocolo de Controle de Transmissão) |
| ToS | *Theft of Service* (Roubo de Serviço) |
| MEC | *Multi-access Edge Computing* (Computação de Borda Multiacesso) |
| NE | *Network Elements* (Elementos de Rede) |
| SEPP | *Security Edge Protection Proxy* (Proxy de Proteção de Borda de Segurança) |
| HPLMN | *Home Public Land Mobile Network* (Rede Móvel Pública Terrestre Residencial) |
| VPLMN | *Visited Public Land Mobile Network* (Rede Pública de Telefonia Móvel Visitada) |
| QBER | *Quantum Bit Error Rate* (Taxa de Erro de Bit Quântico) |
| IR | *Information Reconciliation* (Reconciliação de Informação) |
| COW | *Coherent One-Way* (Coerente Unidirecional) |

| **Sigla** | **Significado** |
|---|---|
| TRNG | *True Random Number Generator* (Gerador de Números Aleatórios Verdadeiros) |
| VPNs | *Virtual Private Networks* (Redes Privadas Virtuais) |
| ESP | *Encapsulating Security Payload* (Encapsulando Carga Útil de Segurança) |
| AH | *Authentication Header* (Cabeçalho de Autenticação) |
| SA | *Security Association* (Associação Segura) |
| SPI | *Security Parameter Index* (Índice de Parâmetros de Segurança) |
| IKE | *Internet Key Exchange* (Troca de Chaves pela Internet) |
| ISAKMP | *Internet Security Association and Key Management Protocol* (Associação de Segurança da Internet e Protocolo de Gerenciamento de Chaves) |
| DH | *Diffie-Hellman* |
| PFS | *Perfect Forward Secrecy* (Sigilo de Encaminhamento Perfeito) |
| SeQKEIP | *Secure Quantum Key Exchange Internet Protocol* (Protocolo de Internet de Troca Segura de Chaves Quânticas) |
| QIKE | *Quantum Internet Key Exchange* (Troca de Chaves de Internet Quântica) |
| SecTAG | *Security Tag* (Etiqueta de Segurança) |
| ICV | *Integrity Check Value* (Valor de Verificação de Integridade) |
| PN | *Package Number* (Número de Pacote) |
| P2P | *Point to Point* (Ponto a Ponto) |
| P2MP | *Point to Multpoint* (Ponto a Multponto) |
| SKR | *Secure Key Rate* (taxas de chave segura) |
| SCI | *Secure Channel Identifier* (Identificador de Canal Seguro) |
| CA | *Connectivity Association* (Associação de Conectividade) |
| MKA | *MACsec Key Agreement* (Acordo de Chave MACsec) |
| MSK | *Master Session Key* (Chave Mestra da Sessão) |
| CAK | *Connectivity Association Key* (Chave de Associação de Conectividade) |
| ASIC | *Application-Specific Integrated Circuit* (Circuito Integrado de Aplicação Específica) |
| ICK | *Integrity Check Key* (Chave de Verificação de Integridade) |
| KEK | *Key Encryption Key* (Chave de Criptografia) |
| SAK | *Secure Association Key* (Chave de Associação Segura) |
| QPN | *Quantum Parameter Monitor* (Monitor de Parâmetros Quânticos) |
| CV-QKD | *Continuous-Variable QKD* (QKD de Variável Contínua) |

| **Sigla** | **Significado** |
|---|---|
| SCI | *Secure Channel Identifier* (Identificador de Canal Seguro) |
| PN | *package number* (Número do Pacote) |

# Lista de Figuras

# Lista de Tabelas

# Capítulo 1

# Introdução

Com o avanço da computação e das redes de comunicação, a segurança tornou-se um dos pilares fundamentais da sociedade digital, especialmente diante da expansão das redes de quinta geração (5G) e do aumento significativo de ciberataques. A criptografia, principal mecanismo de proteção de dados, desempenha papel crucial na garantia da privacidade e integridade das informações. Entretanto, os métodos tradicionais de criptografia, baseados em complexidade computacional, encontram-se ameaçados pelo avanço da computação quântica, um paradigma de processamento capaz de resolver problemas matemáticos complexos em tempos muito reduzidos, comprometendo algoritmos amplamente utilizados [Mehic *et al.* 2024]. Essa vulnerabilidade representa um risco relevante para as redes 5G, que exigem soluções de segurança robustas, escaláveis e de baixa latência [Mehic *et al.* 2024].

O desenvolvimento das redes 5G, com capacidade de suportar altas taxas de transmissão e tempos de resposta reduzidos, trouxe avanços expressivos para a comunicação móvel [Mehic *et al.* 2024]. Contudo, a ampliação da superfície de ataque, decorrente do crescimento de dispositivos conectados, requer novas abordagens para proteção dos dados trafegados [Mehic *et al.* 2024]. Nesse cenário, a criptografia quântica surge como uma alternativa promissora, oferecendo segurança fundamentada em princípios da física quântica e, portanto, resistente às ameaças provenientes da computação quântica.

A Distribuição de Chaves Quânticas (*Quantum Key Distribution – QKD*) aplica propriedades da mecânica quântica para estabelecer e distribuir chaves criptográficas de forma segura entre dispositivos geograficamente distantes [Mehic *et al.* 2024]. Essa técnica é particularmente relevante para redes 5G, que demandam proteção contra interceptações e espionagem em segmentos críticos, como o *fronthaul* óptico (o trecho da rede que conecta as estações rádio-base à unidade central de processamento) [Mehic *et al.* 2024]. Além disso, soluções baseadas em QKD vêm sendo estudadas para aplicações em infraestruturas críticas, redes de Internet das Coisas (IoT) e Internet Industrial das Coisas (IIoT), ampliando as perspectivas de uso.

Dessa forma, este trabalho tem como objetivo analisar o artigo *Quantum Cryptography in 5G Networks: A Comprehensive Overview* [Mehic *et al.* 2024], destacando as aplicações,

desafios técnicos e perspectivas futuras da integração da QKD em redes 5G, bem como a importância de criptografadores dedicados (dispositivos de hardware especializados em gerar e aplicar chaves criptográficas com alta velocidade e baixa latência) para atender aos requisitos de segurança dessas redes.

## 1.1 Justificativa e Relevância do Trabalho

A escolha deste tema se justifica pela crescente preocupação com a segurança da informação em um cenário tecnológico cada vez mais conectado e dinâmico. A evolução e a ampla adoção das redes 5G ampliam significativamente a quantidade e a diversidade de dispositivos conectados, aumentando a superfície de ataque e a complexidade dos mecanismos de proteção. Paralelamente, o avanço da computação quântica coloca em risco algoritmos criptográficos amplamente utilizados, uma vez que computadores quânticos suficientemente desenvolvidos poderão quebrar esquemas como RSA (*Rivest-Shamir-Adleman*) e ECC (*Elliptic Curve Cryptography*) em um tempo muito reduzido.

Nesse contexto, a criptografia quântica, especialmente por meio da *QKD*, surge como uma alternativa promissora, oferecendo garantias de segurança fundamentadas nas leis da física quântica. Essa tecnologia já vem sendo estudada e aplicada em ambientes de alta criticidade, como redes governamentais, bancárias e industriais, e demonstra potencial para proteger segmentos críticos das redes 5G, como enlaces ópticos no *fronthaul*.

O presente trabalho se mostra relevante ao analisar as aplicações e limitações da *QKD* no contexto de redes 5G, com base em um estudo de referência na área. Assim, contribui para a compreensão das oportunidades e dos desafios envolvidos na incorporação da criptografia quântica em arquiteturas de telecomunicações, oferecendo subsídios técnicos para a construção de redes mais seguras e resilientes diante das ameaças emergentes da era quântica.

## 1.2 Objetivos

Esta seção apresenta os objetivos que guiaram a realização deste trabalho. Primeiro, é mostrado o objetivo geral, seguido dos objetivos específicos, que detalham os passos pensados para alcançar o que se propõe.

### 1.2.1 Objetivo Geral

Este trabalho tem como objetivo identificar e analisar as principais soluções de segurança aplicadas em redes 5G com o uso da criptografia quântica, especialmente por meio da técnica da *QKD*, destacando seus benefícios, limitações e potenciais aplicações práticas, como a proteção de enlaces ópticos em ambientes de baixa latência.

### 1.2.2 Objetivos Específicos

a) Compreender a importância da criptografia quântica no contexto da segurança da informação frente aos avanços da computação quântica;

b) Analisar a arquitetura e a organização das redes 5G, considerando suas camadas, funcionamento e implicações para a segurança;

c) Identificar os principais desafios de segurança enfrentados pelas redes 5G, especialmente no cenário de múltiplos dispositivos e baixa latência;

d) Investigar, com base no artigo *Quantum Cryptography in 5G Networks: A Comprehensive Overview*, a viabilidade da integração da QKD em redes 5G, considerando também suas possíveis aplicações práticas, como em enlaces *fronthaul*.

## 1.3 Organização do Documento

Este trabalho está estruturado em quatro capítulos, além da seção de referências, organizados da seguinte forma:

a) **Capítulo 1 – Introdução:** apresenta o tema da pesquisa, a justificativa e sua relevância, além dos objetivos geral e específicos. Também contextualiza a importância da segurança em redes 5G diante do avanço da computação quântica.

b) **Capítulo 2 – Fundamentação Teórica:** descreve os principais conceitos relacionados ao tema, incluindo aspectos de redes 5G, segurança em redes, fundamentos da *QKD*, protocolos como BB84, limitações e pós-processamento, integração com IPsec e MACsec, criptografadores baseados em FPGA, padrões *QKD* e aplicações práticas em redes 5G, com estudos de caso e trabalhos correlatos.

c) **Capítulo 3 – Materiais e Métodos:** apresenta o método de análise utilizado, com base no artigo *Quantum Cryptography in 5G Networks: A Comprehensive Overview*, detalhando a abordagem adotada para interpretar e organizar os dados e conceitos extraídos.

d) **Capítulo 4 – Conclusão:** apresenta as principais conclusões obtidas a partir do estudo do artigo base, destacando as contribuições da *QKD* para redes 5G, suas limitações técnicas e perspectivas. Também inclui sugestões para trabalhos futuros, como o aprofundamento nos estudos de *QKD* e a análise de técnicas de criptografia pós-quântica.

# Capítulo 2

# Fundamentação Teórica

Esta seção tem como finalidade apresentar os principais conceitos teóricos que sustentam o estudo da criptografia quântica aplicada às redes 5G. Para isso, são discutidas inicialmente as características fundamentais das redes de quinta geração e os novos desafios de segurança que surgem com sua implementação em larga escala. Em seguida, explora-se a criptografia quântica, com ênfase na *QKD*, destacando seus fundamentos físicos, potencial de aplicação e limitações práticas. A compreensão desses elementos é essencial para avaliar a viabilidade e a relevância da integração da criptografia quântica como mecanismo de segurança para ambientes de comunicação móvel avançados.

## 2.1 Introdução à Rede 5G

A tecnologia 5G, ou quinta geração de redes móveis, representa um marco significativo na evolução das comunicações sem fio, trazendo avanços expressivos em relação às gerações anteriores. Com taxas de transmissão que podem ultrapassar 10 Gbps [International Telecommunication Union 2020], latências reduzidas a menos de 1 ms e capacidade aprimorada para suportar um grande número de dispositivos conectados simultaneamente, o 5G é projetado para atender às demandas de um mundo cada vez mais digital e interconectado. Essas características permitem uma ampla gama de aplicações, desde comunicações ultra-rápidas até a automação de processos industriais e a implementação de cidades inteligentes.

Além das aplicações funcionais, a arquitetura do 5G é composta por três principais camadas: a Rede de Acesso por Rádio (*Radio Access Network* - RAN), o Núcleo da Rede (*5G Core* - 5GC) e a Rede de Transporte. Essa estrutura modular permite a segmentação lógica da rede, oferecendo suporte simultâneo a diferentes serviços com requisitos diversos, além de possibilitar maior escalabilidade, flexibilidade e eficiência no gerenciamento do tráfego de dados.

A arquitetura do 5G é organizada em três principais cenários de aplicação, conforme ilustrado na Figura 2.1. A representação foi elaborada com base no artigo de referência em [Chowdhury 2020].

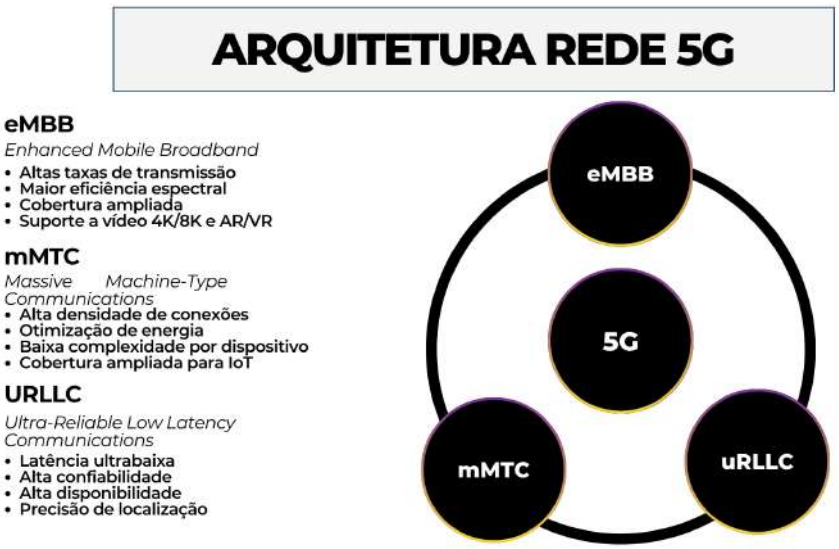



**Figura 2.1:** *Arquitetura simplificada da rede 5G, elaborada com base em [Chowdhury 2020].*

a) *Enhanced Mobile Broadband* (Banda larga móvel aprimorada - eMBB): focado em melhorar a experiência do usuário com altas velocidades de transmissão de dados, ideal para aplicações como streaming de vídeo em alta definição e realidade virtual.

b) *Ultra-Reliable Low Latency Communications* (Comunicações de baixa latência ultra-confiáveis - URLLC): essencial para aplicações críticas que exigem confiabilidade extrema e baixa latência, como cirurgias remotas, veículos autônomos e controle de infraestruturas críticas.

c) *Massive Machine-Type Communications* (Comunicações Massivas do Tipo Máquina - mMTC): projetado para conectar até 1 milhão de dispositivos IoT, permitindo a comunicação em larga escala entre sensores, dispositivos inteligentes e sistemas automatizados.

A expansão das redes 5G também traz desafios significativos, especialmente em relação à segurança. O aumento da superfície de ataque, a diversidade de dispositivos conectados e a necessidade de novas abordagens para proteção de dados tornam a criptografia um componente essencial para garantir a privacidade e a integridade das comunicações [Mehic *et al.* 2024]. Entretanto, os métodos tradicionais de criptografia baseados em complexidade computacional tornam-se cada vez mais vulneráveis diante do avanço iminente da computação quântica. Nesse contexto, cresce a preocupação de que algoritmos criptográficos atualmente utilizados possam ser quebrados em poucos minutos, comprometendo a segurança de dados e sistemas digitais.

Diante desse cenário, soluções inovadoras como a criptografia quântica despontam como alternativas promissoras para fortalecer a segurança das redes 5G. A *QKD*, por exemplo, utiliza princípios da física quântica para estabelecer chaves criptográficas de forma segura e resistente à espionagem [Mehic *et al.* 2024]. Essa tecnologia é particularmente relevante

para aplicações críticas, como redes *IoT* e infraestruturas de energia, nas quais a segurança dos dados é fundamental.

### 2.1.1 Arquitetura da Rede 5G

A arquitetura de rede 5G difere da 4G em vários aspectos significativos. O 5G apresenta uma arquitetura dividida, que incorpora recursos de desempenho, gerenciamento de carga, otimização e adaptabilidade a diversas aplicações. Implementações flexíveis de *hardware* e *software* possibilitam implantações de rede escaláveis, mesmo quando diferentes fornecedores fornecem componentes de *hardware* e *software* 3GPP (2020, apud [Mehic *et al.* 2024]).

A Rede de Acesso por Rádio (*Radio Access Network* - RAN) é frequentemente denominada segmento de rede *fronthaul*. Esse componente supervisiona a comunicação com o Equipamento do Usuário (*User Equipment* - UE). Em gerações anteriores de redes móveis, a estação base era alojada em uma única unidade física, resultando em uma estrutura distribuída. No entanto, os avanços na fabricação de componentes eletrônicos permitiram a consolidação de vários blocos de comunicação de rádio em um único dispositivo. Tornou-se então viável que uma única unidade operasse com diversas antenas de *Radio Frequency* (RF), introduzindo a noção de uma arquitetura centralizada, conhecida como *Cloud Radio Access Network* (C-RAN). As estações base contêm uma unidade de processamento digital de rádio, denominada Unidade Distribuída (*Distributed Unit* - DU) ou Unidade de Banda Base (*Baseband Unit* - BBU), que alimenta as diversas unidades operacionais de RF na arquitetura 5G, chamadas de Cabeça de Rádio Remota (*Remote Radio Head* - RRH) ou Unidade de Rádio Remota (*Remote Radio Unit* - RRU), também conhecidas simplesmente como Unidade de Rádio (*Radio Unit* - RU).

A BBU é responsável por processar sinais de banda base (sinais antes da modulação) por meio da interface física para a rede principal. A RRU é composta por diversas unidades de processamento RF e antenas de estação de rádio. Para atingir altas velocidades de comunicação entre as unidades BBU, localizadas em um Escritório Central (*Central Office* - CO) seguro, e a RRU externa, utiliza-se conectividade óptica. Contudo, essa conexão é limitada a algumas dezenas de quilômetros para satisfazer as restrições de tempo da tecnologia de rádio. O protocolo de Solicitação de Repetição Automática Híbrida (*Hybrid Automatic Repeat Request* - HARQ) é geralmente empregado como mecanismo de retransmissão entre o UE e a RRU, com um tempo de processamento na DU inferior a 3 ms. Para reduzir o tempo de propagação da fibra e atender aos requisitos do HARQ, a conexão *fronthaul* entre a RRU e a BBU deve ser implantada a uma distância de aproximadamente 20 km, dependendo da implementação da RAN [Larsen, Checko e Christiansen 2018; 3GPP 2020; Al-obaidi *et al.* 2015]. Nas seções seguintes, discute-se essa limitação, que favorece o uso de links *QKD*, os quais também apresentam restrições de comprimento.

O *midhaul* refere-se a um conjunto de links que conectam os segmentos *fronthaul* e *backhaul* [Mehic *et al.* 2024]. A evolução do 5G com o conceito de *Open-RAN* modificou a

estrutura da arquitetura BBU e RRH desenvolvida para redes 4G, dividindo a BBU em uma DU e uma Unidade Centralizada (*Centralized Unit* - CU). Algumas funcionalidades clássicas da BBU, incluindo as subcamadas PHY, MAC e RLC, permanecem na DU, enquanto outras são movidas para a CU. Esse tipo de configuração requer que o *fronthaul* possibilite comunicação simultânea. Isso também implica que o link *fronthaul* para as RUs seja a única conexão que se estende além da infraestrutura física das operadoras de telecomunicações e, como tal, sua segurança deve ser abordada de forma específica. A opção mais amplamente utilizada para links *fronthaul* é o *Enhanced Common Public Radio Interface* (eCPRI), desenvolvido para acelerar as comunicações entre a RRU e a DU. Dependendo da disponibilidade de transporte e da interface *fronthaul*, a DU e o software associado podem ser hospedados localmente ou em uma nuvem de ponta (*edge cloud* ou centro de dados).

A seção de *backhaul* ilustrada no esquema da Figura 2.2 representa a rede entre a UC e o núcleo 5G. Por estar localizada profundamente dentro do perímetro de segurança da operadora de telecomunicações, essa parte da rede permite a aplicação de diversas soluções baseadas em computação quântica, com o objetivo de elevar o nível de segurança das comunicações.

A Figura 2.2 ilustra o orçamento de latência do tempo de ida e volta (*round trip time* - RTT) na comunicação entre a UE, as RRUs e a DU, interligadas pelo enlace *fronthaul* óptico via interface eCPRI. O esquema mostra que o protocolo HARQ deve respeitar um limite máximo de 3 ms, o que impõe restrições de distância entre a DU e as RRUs. Esse intervalo inclui tanto o tempo de transmissão quanto o de processamento interno dos nós de rede. Caso a distância ou a latência exceda o limite, o mecanismo de retransmissão (NACK) não funcionará de forma eficiente, comprometendo a qualidade do enlace. Por isso, a conexão *fronthaul* é um ponto crítico da arquitetura 5G e também um candidato relevante para a aplicação de mecanismos de segurança baseados em QKD, que enfrentam restrições semelhantes de alcance físico.

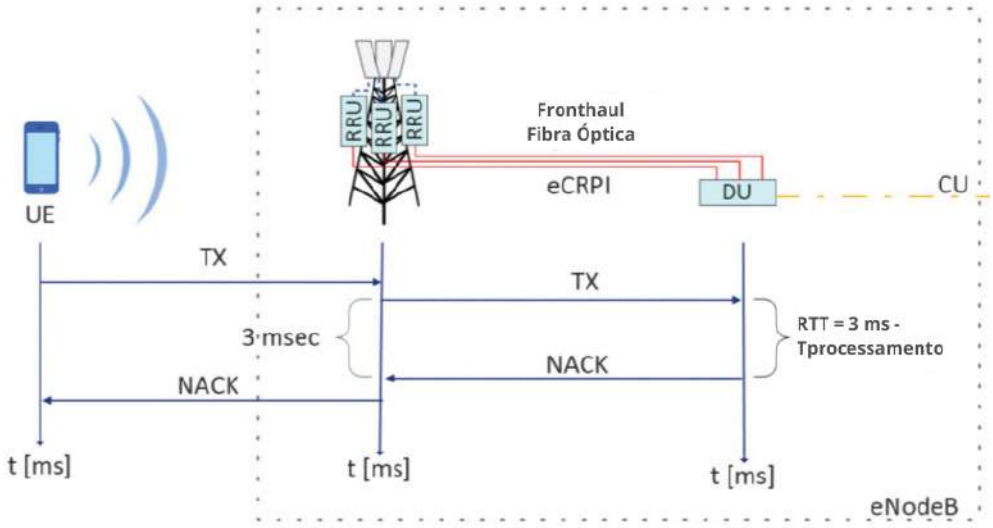



**Figura 2.2:** *Orçamento de link de latência do RTT da camada MAC em C-RAN. Fonte: Adaptado de Quantum Cryptography in 5G Network [Mehic* et al. *2024].*

A seguir, apresenta-se uma visão geral sistemática da arquitetura 5G, discutem-se problemas de segurança identificados e são apresentados métodos de integração de técnicas de *QKD* para fortalecimento da segurança.

### 2.1.2 Segurança em Redes 5G

As redes 5G são consideradas facilitadoras essenciais para atender às crescentes demandas de aplicações sem fio emergentes, fornecendo altas taxas de dados e latência ultrabaixa para uma ampla variedade de dispositivos com conectividade onipresente [Ahmad *et al.* 2018; Yang *et al.* 2015]. Dessa forma, as redes 5G transmitirão quantidades extremamente grandes de dados confidenciais e sensíveis. A segurança, portanto, torna-se uma questão crítica no projeto, implantação e uso dessas redes [Wu *et al.* 2018].

Os mecanismos de segurança introduzidos nas redes 2G foram projetados principalmente para garantir o correto funcionamento dos sistemas de faturamento, por meio de autenticação de usuário unidirecional, além de fornecer integridade e confidencialidade de dados pela RAN [Mehic *et al.* 2024]. Consequentemente, as redes 2G eram vulneráveis a *spam* e a ataques de falsificação de Estação Base (*Base Station* - BS), enquanto a confidencialidade e a integridade dos dados transmitidos estavam em risco devido ao uso de cifras de fluxo fracas [Mehic *et al.* 2024].

No 3G, a autenticação bidirecional foi habilitada para eliminar ataques falsos de BS. Apesar disso e do fato de o 3G ter introduzido algoritmos de criptografia mais robustos do que o 2G, essas redes ainda eram vulneráveis a espionagem, personificação de assinante

e rede, ataques *Man-in-the-Middle* (MitM), *Denial of Service* (DoS) e outras ameaças de segurança cibernética.

Com o 4G, foram introduzidos algoritmos criptográficos avançados e mecanismos de autenticação aprimorados, como o protocolo de Autenticação e Acordo de Chave (*Authentication and Key Agreement* - AKA), juntamente com o *Internet Protocol Security* (IPsec), projetado para proteger o tráfego dentro da rede central. No entanto, o caráter totalmente baseado em IP das redes 4G as expôs a novas ameaças típicas da Internet, como falsificação de endereço IP, ataques DoS SYN do *Transmission Control Protocol* (TCP), roubo de identidade do usuário, roubo de serviço (*Theft of Service* - ToS) e ataques de intrusão.

Para mitigar parte desses problemas, o 5G introduziu novos recursos de segurança, como a proteção da identidade do usuário em links de rádio, a proteção da integridade do plano do usuário na interface de rádio e a autenticação do equipamento do usuário em redes domésticas quando uma rede de servidores não confiável é acessada. Apesar desses avanços, o 5G herda a maioria das vulnerabilidades baseadas em IP do 4G e ainda enfrenta desafios adicionais devido à necessidade de oferecer suporte a um número extremamente elevado de dispositivos heterogêneos e aplicações de missão crítica [Mehic *et al.* 2024].

Na segunda etapa da migração para fornecer redes 5G SA, o núcleo legado também exigiu modificações para permitir uma arquitetura baseada em serviços, possibilitando uma separação mais clara entre os planos de controle e de usuário. Para esse fim, o 3GPP introduziu a definição da rede por software por meio do uso de novas tecnologias [Ahmad *et al.* 2018; Khan *et al.* 2020; Arfaoui *et al.* 2018]:

a) Redes definidas por software (*Software-Defined Networking* - SDN), que permitem a softwareização das funções de rede ao desacoplar os planos de controle e de dados e possibilitar a programação em ambos os planos;

b) Virtualização de funções de rede (*Network Functions Virtualization* - NFV), que desacopla funções de rede de hardware proprietário e as executa como instâncias de software;

c) Computação em nuvem e computação de ponta multiacesso (*Multi-access Edge Computing* - MEC), que fornecem escalabilidade sob demanda para redes, reunindo sistemas tecnologicamente distintos em um único domínio onde vários serviços podem ser implantados;

d) Fatiamento de rede, que aprimora o suporte para diferentes classes de tráfego em redes 5G, permitindo que a infraestrutura de rede compartilhe os mesmos recursos para múltiplos usos.

Embora úteis, essas tecnologias apresentam desafios de segurança próprios. Para mitigar esses e outros problemas, o 3GPP fornece diretrizes específicas para autenticação, autorização, confiança e gerenciamento de identidade em redes 5G. A arquitetura de segurança 3GPP

5G pode ser considerada uma coleção de várias funções de rede, protocolos e componentes responsáveis pela segurança de ponta a ponta, protegendo o controle e o tráfego do usuário dentro da RAN e da Rede Central 5G (5GC) (*fronthaul* e *backhaul*), além de assegurar as comunicações entre redes domésticas e de visitantes [Mehic *et al.* 2024].

Os principais mecanismos de segurança 5G são:

a) Controle de acesso da UE, obtido pela aplicação de autenticação bidirecional entre o usuário e a rede;

b) Proteção da identidade do usuário, confidencialidade dos dados e integridade da interface via aérea, alcançadas respectivamente pela aplicação de criptografia assimétrica, criptografia simétrica e algoritmos de hash;

c) Comunicações seguras entre elementos de rede 5G (*Network Elements* - NE), obtidas pela aplicação de HTTPS entre funções de serviço 5GC isoladas e IPsec para garantir a segurança das informações para o *Security Edge Protection Proxy* (SEPP) entre a rede móvel terrestre pública residencial *(Home Public Land Mobile Network* - HPLMN) e a rede móvel terrestre pública visitante (*Visited Public Land Mobile Network* - VPLMN).

## 2.2 Introdução a Distribuição de Chaves Quânticas

Em 1984, Charles Bennett e Gilles Brassard apresentaram um conceito inovador de comunicação segura baseado na mecânica quântica [Bennett e Brassard 1984; Bennett e Brassard 1984], para ilustrar como fenômenos quânticos podem alavancados para estabelecer um canal de comunicação (ou seja, um canal quântico) do qual as informações não podem ser lidas ou copiadas de forma confiável. Qualquer tentativa de escuta passiva no canal quântico pode também ser detectada com alta probabilidade. As características de transferências de informações através de sistemas quânticos elementares, por exemplo fótons polarizados, são garantidos pelas leis da mecânica quântica através da incerteza de Heisenberg e do teorema de não clonagem. Bennet e Brassard também descreveram um esquema, agora conhecido como protocolos BB84, para permitir a distribuição de chaves simétricas entre duas partes distantes, tradicionalmente chamados de Alice e Bob, desde que tenham um canal público autenticado à sua disposição além do quântico. Em 1989, Bennet e Brassard provaram sua ideia experimentalmente no primeiro experimento *QKD* a uma distância de 32.5 centímetros no espaço livre Bennett e Brassard (1989, apud [Mehic *et al.* 2024]). Este experimento estimulou o interesse na integração e aplicação mais ampla da tecnologia, que está presente hoje [Mehic *et al.* 2024]. A topologia de uma rede *QKD* é ilustrada na Figura 2.3.

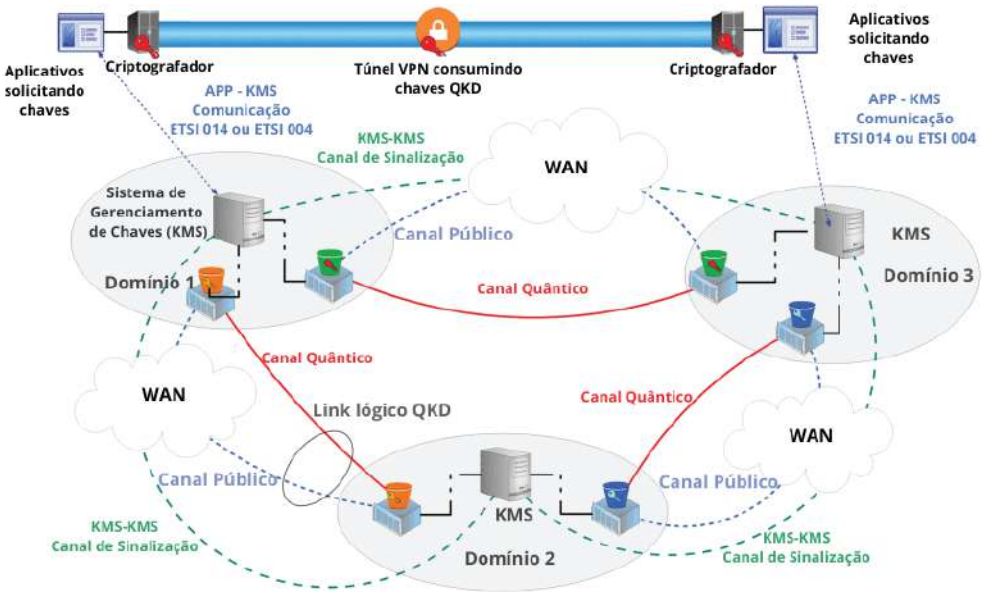



**Figura 2.3:** *A conexão lógica dos links QKD. Essas conexões consistem em um canal quântico óptico (linha vermelha contínua) e um canal público/clássico (linha azul pontilhada). Uma rede QKD consiste em múltiplos links QKD e sistemas Key Management Systems - (KMS) que fornecem chaves para aplicações do usuário final. Os criptografadores consomem as chaves fornecidas para estabelecer uma comunicação de dados segura. Fonte: Adaptado de Quantum Cryptography in 5G Network [Mehic* et al. *2024].*

A Figura 2.3 apresenta a topologia de uma rede *QKD*. Cada enlace é composto por dois canais: o canal quântico (em vermelho), utilizado para a transmissão de fótons que carregam a informação da chave, e o canal público/clássico (em azul pontilhado), que é autenticado e permite a comunicação auxiliar entre os nós. Os Sistemas de Gerenciamento de Chaves KMS são responsáveis por receber as chaves geradas pelos enlaces quânticos, armazená-las e distribuí-las para aplicações seguras. Nessas aplicações, os criptografadores consomem as chaves fornecidas para estabelecer túneis VPN de alta segurança. Assim, a rede QKD opera como uma camada de infraestrutura de segurança, capaz de interconectar diferentes domínios e fornecer chaves de forma contínua e escalável para diversos serviços críticos.

### 2.2.1 O Protocolo BB84

O protocolo BB84, proposto por Bennett e Brassard em 1984 [Bennett e Brassard 1984], é amplamente reconhecido como o primeiro esquema prático de *QKD*. Seu funcionamento baseia-se na codificação de informações binárias em estados quânticos de fótons, cuja polarização é manipulada de forma controlada. O processo ocorre entre dois participantes fictícios, tradicionalmente chamados de Alice (emissora) e Bob (receptor), utilizando dois canais distintos: um quântico, para a transmissão de fótons, e outro clássico, para comunicação pública autenticada.

Alice prepara e envia uma sequência de fótons com polarizações escolhidas aleatoriamente entre duas bases ortogonais: retilínea (com ângulos de 0° e 90°) e diagonal (com 45° e 135°). Cada base representa duas possibilidades de polarização, e, portanto, cada fóton carrega um

bit de informação. Bob, ao receber cada fóton, também escolhe aleatoriamente qual base utilizará para realizar a medição, sem saber previamente qual foi usada por Alice. Devido ao princípio da incerteza de Heisenberg, não é possível medir com precisão o estado de polarização se a base de medição for incompatível com a base de preparação.

Neste contexto do protocolo BB84, bases de preparação referem-se às orientações escolhidas por Alice para preparar os fótons que representarão os bits. Existem duas bases possíveis: a retilínea (com polarizações em 0° e 90°) e a diagonal (com polarizações em 45° e 135°). Cada base é composta por dois estados ortogonais que podem codificar os valores lógicos 0 e 1. Já as bases de medição correspondem às escolhas de Bob ao medir os fótons recebidos. Como Bob não sabe de antemão qual base foi utilizada por Alice, ele também seleciona entre a base retilínea e a base diagonal de forma aleatória. Quando a base de medição coincide com a base de preparação, o resultado obtido corresponde ao bit enviado; quando são diferentes, o resultado da medição é aleatório e, portanto, descartado na fase de peneiramento (*sifting*).

Nas situações em que a escolha de Bob coincide com a base utilizada por Alice, ele obtém o valor correto do bit. Caso contrário, o resultado é aleatório. Após a transmissão, Alice e Bob utilizam o canal clássico para comparar quais bases foram utilizadas, sem revelar os bits em si. Eles então descartam todos os bits correspondentes às medições feitas com bases divergentes, processo conhecido como *sifting* (ou peneiramento), resultando em uma sequência parcialmente compartilhada, chamada de chave peneirada.

A Figura 2.4 apresenta as duas bases de polarização utilizadas no protocolo BB84: a retilínea (0° e 90°) e a diagonal (45° e 135°). Cada fóton transmitido por Alice pode representar o valor lógico 0 ou 1, dependendo da polarização escolhida. Essa codificação quântica garante que a tentativa de medir um fóton em uma base incorreta introduza incertezas e erros, característica essencial para a segurança do protocolo.

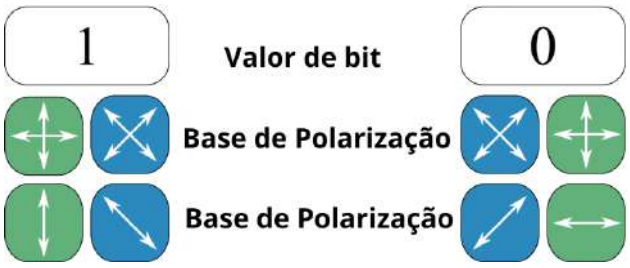



**Figura 2.4:** *Esquema de codificação no protocolo BB84. Fonte: Adaptado de Quantum Cryptography in 5G Network [Mehic* et al. *2024].*

A Figura 2.5 apresenta de forma esquemática as etapas iniciais do protocolo BB84 de distribuição quântica de chaves. Na primeira linha, Alice define uma sequência aleatória de bits; na segunda, escolhe aleatoriamente as bases de polarização (reta ou diagonal) para cada bit; e na terceira, codifica essa informação em fótons com as polarizações correspondentes. Na quarta linha, Bob mede cada fóton utilizando também bases de medição escolhidas aleatoriamente. Na quinta, após a transmissão, Alice e Bob comparam em um canal clássico

quais bases foram iguais, identificando os casos em que a medição foi válida; na sexta, esses resultados compatíveis são destacados; e, finalmente, na sétima linha, forma-se a chamada chave peneirada (*sifted key*), que consiste apenas nos bits obtidos quando as bases coincidiram e que servirá de base para as etapas seguintes de correção de erros e amplificação de privacidade.

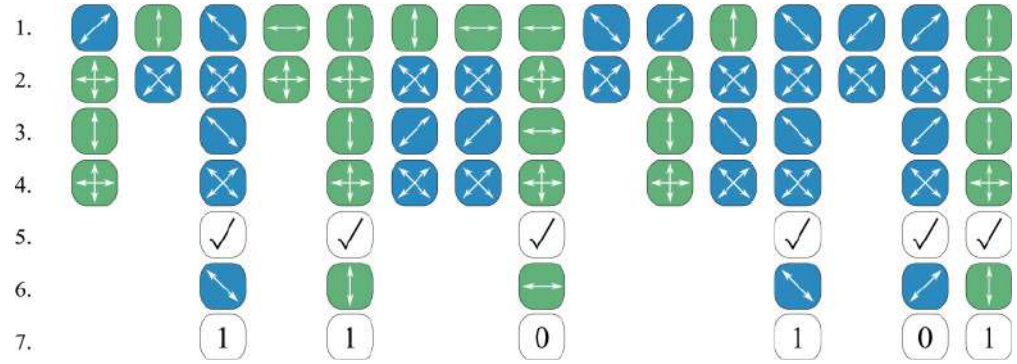



**Figura 2.5:** *Fig. 9. Fluxo resumido do protocolo BB84, abrangendo a transferência quântica e a fase de peneiramento: (1) Alice envia uma sequência aleatória de fótons polarizados; (2) Bob mede a polarização dos fótons utilizando uma sequência aleatória de bases; (3) Alguns fótons podem não ser recebidos; (4) Bob anuncia publicamente a base utilizada para cada fóton recebido; (5) Alice informa quais medições estavam corretas; (6) Alice e Bob descartam os resultados correspondentes às medições incompatíveis; (7) Os dados restantes formam a chave peneirada, que é idêntica para Alice e Bob em condições ideais (ver Fig. 8 para o esquema de codificação). Fonte: Adaptado de Quantum Cryptography in 5G Network [Mehic* et al. *2024].*

Na prática, o canal quântico pode estar sujeito a perdas, ruídos e tentativas de interceptação. Isso significa que a sequência obtida por Bob, mesmo após o peneiramento, pode conter erros em relação à de Alice. Para tratar essas discrepâncias, os dois participantes realizam uma etapa de correção de erros por meio do canal público, chamada Reconciliação de Informações (*Information Reconciliation* - IR). Durante essa fase, utilizam-se protocolos como *Cascade* ou LDPC, capazes de alinhar as sequências sem revelar diretamente os bits envolvidos.

Em seguida, com o objetivo de minimizar qualquer possível conhecimento obtido por um espião, aplica-se a Amplificação da Privacidade (*Privacy Amplification*). Essa etapa reduz o tamanho da chave final, transformando a sequência reconciliada em uma nova chave mais curta, porém com alta garantia de sigilo. O processo considera a Taxa de Erro de Bit Quântico (*Quantum Bit Error Rate* - QBER), estimada pela comparação de uma amostra pública da chave peneirada. Caso a QBER esteja dentro de limites aceitáveis (considerando imperfeições do meio físico), a chave final pode ser considerada segura; do contrário, todo o processo é descartado e reiniciado.

Todas as etapas subsequentes à transmissão quântica, como peneiramento, reconciliação e amplificação da privacidade são denominadas coletivamente como pós-processamento do protocolo BB84. Essa sequência de operações garante que, mesmo na presença de ruído ou observadores não autorizados, uma chave secreta e segura possa ser compartilhada entre as

partes.

### 2.2.2 Limitações do *QKD*

Embora a *QKD* ofereça promissoras garantias de segurança baseadas em princípios da física quântica, sua implementação prática enfrenta limitações significativas que impactam sua viabilidade em ambientes de rede reais. Entre os principais desafios estão vulnerabilidades tecnológicas que abrem margem para ataques específicos. A literatura já descreve ataques bem-sucedidos a sistemas *QKD*, como o *Photon Number Splitting*, o ataque do *Cavalo de Troia* e os chamados *Faked States*, todos explorando deficiências em componentes ópticos e emissores de fótons imperfeitos [Huttner *et al.* 1995; Bethune e Risk 2000; Makarov e Hjelme 2005; Gisin *et al.* 2002].

Felizmente, a maioria desses ataques pode ser mitigada por meio de contramedidas técnicas e aperfeiçoamento dos dispositivos, o que reforça a necessidade de pesquisa contínua no campo da engenharia de segurança quântica. Ainda assim, há obstáculos inerentes às características físicas do canal quântico, principalmente no que se refere à relação inversa entre distância e taxa de geração de chaves. Em geral, taxas mais altas são obtidas apenas em distâncias mais curtas. Sistemas atuais conseguem gerar apenas algumas centenas de kilobits por segundo em distâncias próximas a 100–150 km [Mehic *et al.* 2024], o que limita aplicações que demandem alta largura de banda ou autenticação frequente.

Essas restrições inviabilizam, por exemplo, o uso prático do esquema *One-Time Pad* (OTP) em redes modernas, já que a quantidade de chave gerada não acompanha o volume de dados trafegado. Em função disso, o uso do *QKD* costuma ser combinado com algoritmos simétricos resistentes a ataques quânticos, formando uma arquitetura híbrida de segurança. Contudo, alguns especialistas questionam se essa abordagem realmente supera as soluções baseadas exclusivamente em Criptografia Pós-Quântica (*Post-Quantum Cryptography* - PQC), sobretudo quando esta é associada a cifradores simétricos de alta robustez.

Apesar dessas críticas, o *QKD* continua sendo uma tecnologia relevante, especialmente por sua capacidade de oferecer distribuição de chaves com segurança independente de avanços futuros em computação. Em muitas arquiteturas, prevê-se que a geração de chaves possa ocorrer de forma contínua, com armazenamento em *buffers* nos pontos terminais. Isso permitiria responder rapidamente a demandas elevadas, desde que sejam adotadas políticas de gerenciamento e armazenamento seguro de chaves Mehic (2017, apud [Mehic *et al.* 2024]).

Outra limitação crítica diz respeito à vulnerabilidade a ataques de negação de serviço (*Denial of Service* - DoS). Um sistema *QKD* ponto a ponto pode ser comprometido caso o canal quântico seja interrompido por interferências externas ou danos físicos, como cortes na fibra óptica Elliott (2002, apud [Mehic *et al.* 2024]). Nessa circunstância, a interrupção na geração de chaves impossibilita o uso contínuo de canais seguros, exigindo a adoção de alternativas criptográficas convencionais ou a suspensão da comunicação segura até que o serviço seja restabelecido.

### 2.2.3 Abordagens de Pós-Processamento *QKD*

Após a troca inicial de *qubits* por meio do canal quântico, os protocolos de *QKD* avançam para uma etapa crucial chamada pós-processamento. Essa fase, realizada em um canal clássico autenticado, tem como objetivo transformar os dados brutos recebidos em uma chave criptográfica segura e compartilhada entre as partes envolvidas. As etapas típicas desse processo incluem: extração da chave bruta (*sifting*), estimativa da taxa de erro quântico (*QBER*), reconciliação de erros, amplificação da privacidade e autenticação das mensagens trocadas.

A Figura 2.6 apresenta de forma sequencial o procedimento de estabelecimento de chaves. Inicialmente, ocorre a transferência quântica, em que Alice envia fótons preparados em diferentes bases. Em seguida, os bits obtidos são submetidos à peneiração (sifting), na qual Alice e Bob descartam os resultados medidos em bases incompatíveis. Esse conjunto reduzido é então validado por meio de autenticação, seguido da estimativa da taxa de erro (QBER), que permite verificar se houve interferência ou tentativa de espionagem. Caso os erros estejam em limites aceitáveis, aplica-se a reconciliação, que corrige discrepâncias sem expor os bits. Por fim, a amplificação da privacidade reduz ainda mais a chave, garantindo que qualquer possível informação obtida por um espião seja insignificante.

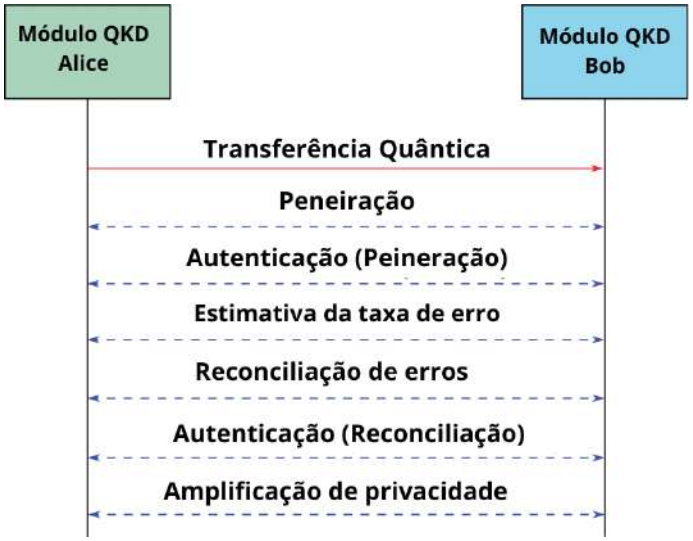



**Figura 2.6:** *Procedimento geral de estabelecimento de chaves em um protocolo QKD. Adaptado de Quantum Cryptography in 5G Network [Mehic* et al. *2024].*

Já a Figura 2.7 demonstra como as chaves geradas no processo anterior podem ser integradas à pilha de protocolos TCP/IP. Nesse contexto, a QKD atua como uma fonte confiável de chaves que pode alimentar diferentes camadas de segurança: no nível da aplicação (TLS/D-TLS), no transporte (VPNs seguras), na camada de rede (IPsec) ou no enlace de dados (MACsec). Assim, a chave quântica estabelecida entre os módulos QKD é distribuída pelos sistemas de gerenciamento de chaves (KMS), permitindo sua utilização em múltiplos pontos da pilha de protocolos.

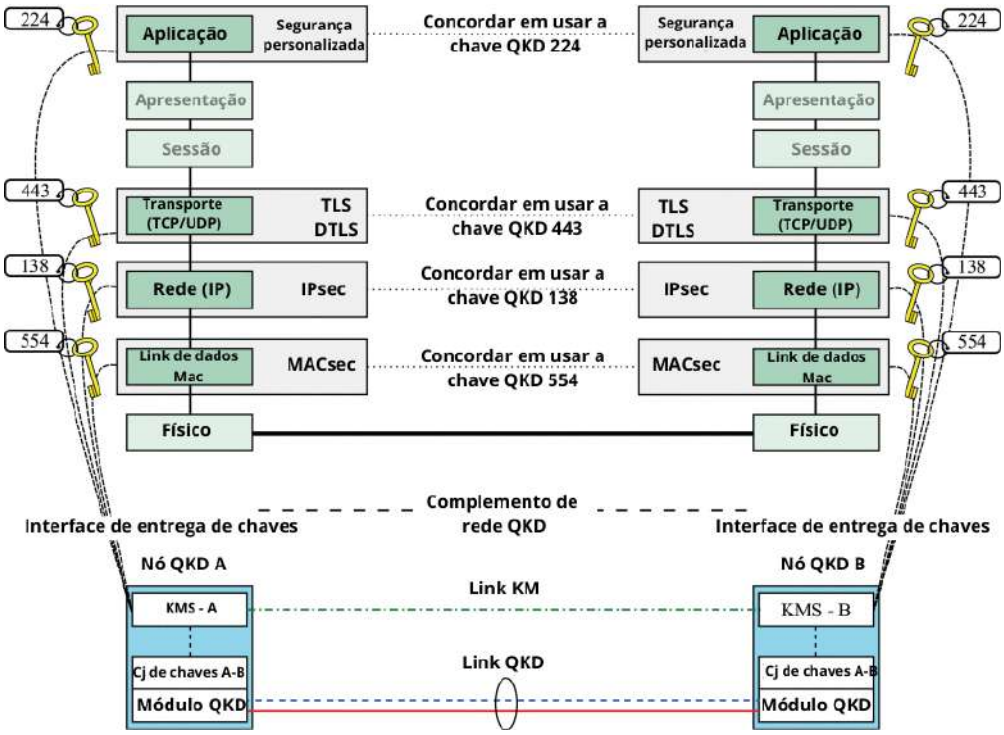



**Figura 2.7:** *Utilização de chaves QKD ou PQC para proteger conexões em diferentes camadas de rede TCP/IP. Adaptado de Quantum Cryptography in 5G Network [Mehic* et al. *2024].*

Historicamente, as etapas de pós-processamento eram implementadas por meio de *software*, utilizando estações de trabalho potentes ou dispositivos dedicados. No entanto, à medida que a camada quântica se tornou mais eficiente, o pós-processamento passou a ser considerado um dos principais gargalos dos sistemas *QKD*. Para superar esse entrave, pesquisas atuais exploram implementações em *hardware*, especialmente em FPGAs *(Field Programmable Gate Arrays)*, que oferecem paralelismo, velocidade e flexibilidade, tornando-se ideais para lidar com o processamento intensivo dessas etapas [Constantin *et al.* 2017; Mehic *et al.* 2017; Mink 2007].

Para superar esse entrave, pesquisadores passaram a explorar implementações em *hardware*, com ênfase em dispositivos reconfiguráveis como os FPGAs. Esses dispositivos oferecem paralelismo, alta velocidade e flexibilidade, sendo ideais para lidar com o processamento intensivo das etapas finais do *QKD*.

A Tabela 2.1 compara diversas implementações de pós-processamento baseadas em FPGA, detalhando suas configurações e as taxas máximas de geração de chaves atingidas.

Um dos trabalhos pioneiros nesse campo é apresentado por Stucki et al. (2007, apud [Mehic *et al.* 2024]), que propuseram o uso do protocolo *Coherent One-Way* (COW) aliado a FPGAs da família *Virtex II Pro*. O sistema alcançou taxas médias de chave secreta em torno de 2,2 kbps, mas apresentou desafios relacionados ao alto índice de erros (QBER), demandando melhorias na detecção.

Outros trabalhos avançaram nesse cenário, como o de Constantin [Constantin *et al.* 2017], foi desenvolvido um sistema completo de destilação de chaves baseado no protocolo COW, implementado em FPGA *Virtex-6*, incluindo todas as fases do pós-processamento.

| Reference | FPGA Platform | Post-processing phase | Clock freq. (MHz) | Max. key rate (Mbps) |
|---|---|---|---|---|
| Damien et al. [102] | Xilinx Virtex II Pro | *sifting, IR, PA* | *unknown* | 0.0022 |
| Zhang et al. [103] | Intel Cyclone III | *sifting, IR, PA* | 40 MHz | 0.07 |
| Constantin et al. [100] | Xilinx Virtex-6 | *sifting, IR, PA* | 125 MHz | 4 |
| Yang et al. [104] | Xilinx Virtex-7 | PA | 100 MHz | 6.4 |
| Yang et al. [105] | Xilinx Virtex-7 | IR, PA | *unknown* | 38.18 |

**Tabela 2.1:** *Comparação de taxa de transferência em mecanismos de pós-processamento QKD baseados em FPGA. Fonte: Quantum Cryptography in 5G Network [Mehic* et al. *2024].*

Essa abordagem se mostrou compacta e eficiente, com destaque para sua independência em relação ao protocolo óptico utilizado.

Visando otimizar a fase de amplificação da privacidade (PA), Yang et al. (2017, apud [Mehic *et al.* 2024]), propuseram uma arquitetura de alto desempenho utilizando FPGA *Virtex-7*. Sua proposta dividia as operações de multiplicação de matrizes em blocos paralelos, elevando significativamente a velocidade de execução dessa etapa crítica.

Complementando essas abordagens, Yang et al. (2020, apud [Mehic *et al.* 2024]) exploraram uma integração entre IR e PA, conseguindo atingir uma taxa de transferência de até 38,18 Mbps com FPGA *Virtex-7*, embora as simulações indicassem um potencial ainda maior.

Esses avanços demonstram que a eficiência do pós-processamento é um fator central para a escalabilidade dos sistemas *QKD*. Melhorias contínuas em *hardware* são essenciais para acompanhar o progresso da camada quântica e viabilizar a adoção prática da criptografia quântica em ambientes exigentes como redes 5G.

### 2.2.4 Redes *QKD*

Melhorias tanto na camada quântica quanto no pós-processamento *QKD* são, sem dúvida, um avanço importante para alcançar taxas de chaves mais altas. No entanto, as aplicações de sistemas *QKD* autônomos são limitadas e fornecem apenas o estabelecimento de chaves simétricas entre dois nós adjacentes em áreas metropolitanas. Sem as tecnologias ainda indisponíveis de repetidores quânticos e relés quânticos [Alleaume 2014; Salvail 2010], uma abordagem diferente foi adotada para expandir o alcance do *QKD*.

Em Elliott (2002, apud [Mehic *et al.* 2024]), os autores introduziram a primeira arquitetura de sistemas para uma rede *QKD* que estendeu o alcance do *QKD* e o fortaleceu contra ataques DoS. Na arquitetura proposta, a chave quântica pode ser retransmitida pela rede *QKD* de maneira salto a salto, permitindo o estabelecimento de chaves simétricas seguras e comprovadas entre dois nós *QKD* arbitrários. No entanto, os nós *QKD* que servem como

relés devem ser confiáveis, pois a chave secreta transitará por eles como texto simples.

Em uma rede $T$-conectada, a retransmissão de chaves pode ser executada com segurança, mesmo que alguns nós *QKD* sejam comprometidos por um espião [Mehic *et al.* 2024]. Isso é possível dividindo a chave secreta em $T$ porções e transmitindo-as por meio de $T$ caminhos nó-disjuntos na rede *QKD*. Nesse caso, um espião precisaria comprometer pelo menos $T$ nós para revelar a chave secreta retransmitida pela rede.

Uma rede *QKD* em malha também é muito mais resiliente a ataques DoS do que sistemas *QKD* independentes, pois a chave secreta pode ser distribuída por vários caminhos diferentes. Redes *QKD* têm sido intensamente pesquisadas, e inúmeros bancos de testes foram implementados nas últimas duas décadas para investigar as possibilidades dessa tecnologia. Uma visão geral recente dos bancos de testes de redes *QKD* existentes é fornecida em Mehic (2020, apud [Mehic *et al.* 2024]).

## 2.3 Integrando *QKD* em Estruturas de Segurança existentes

É amplamente reconhecido que as redes *QKD* têm um propósito específico: gerar, gerenciar e distribuir chaves de forma intrinsecamente segura do ponto de vista da ITS, fornecendo chaves sob demanda como um serviço aos consumidores [Dianati e Alléaume 2007]. As redes *QKD* são, portanto, comumente consideradas uma tecnologia suplementar destinada a aprimorar a segurança de sistemas de comunicação já existentes.

Entretanto, por atuarem essencialmente como uma fonte confiável de chaves criptográficas, e não como uma solução completa de comunicação quântica segura, essas redes precisam ser integradas a arquiteturas de segurança já consolidadas para que possam oferecer proteção efetiva no contexto de redes modernas.

Dessa forma, esta seção examina como os serviços de rede *QKD* , especificamente as chaves seguras que elas geram e fornecem , podem ser utilizados para fortalecer a privacidade e a segurança em conceitos e protocolos de comunicação segura amplamente conhecidos.

### VPNs Baseadas em QKD

A convergência da tecnologia *QKD* depende diretamente de sua aceitação e integração com as redes IP amplamente difundidas atualmente. Nesse contexto, técnicas consolidadas de redes privadas virtuais (*Virtual Private Networks* – VPNs) para comunicação segura em redes IP têm sido expandidas para suportar chaves geradas por *QKD*.

Esta seção examina, em especial, a integração da *QKD* com o protocolo IPsec, considerado a técnica mais popular e amplamente utilizada para estabelecer conexões VPN seguras em redes IP modernas.

Além do IPsec, o protocolo *Media Access Control Security* (MACsec) também tem ganhado relevância em determinadas aplicações, principalmente devido à sua simplicidade, ao

suporte a taxas de linha e à baixa latência, características essenciais para cenários de alta demanda de desempenho.

### Segurança do Protocolo de Internet (IPsec)

O IPsec define uma arquitetura de segurança que fornece proteção para comunicações na Internet na camada de rede. Os serviços de segurança oferecidos incluem controle de acesso, integridade de dados, autenticação da origem, confidencialidade do conteúdo transmitido e proteção contra ataques de repetição Kent e Atkinson (1998, apud [Mehic *et al.* 2024]).

Para oferecer esses serviços, o IPsec utiliza dois protocolos principais: o *Encapsulating Security Payload* (ESP) e o *Authentication Header* (AH). O AH assegura integridade e autenticação, mas não realiza criptografia, enquanto o ESP garante também a confidencialidade dos dados transmitidos.

Além disso, o IPsec pode operar em dois modos distintos:

a) **Modo transporte**: protege apenas os dados da camada superior (como TCP/UDP), mantendo o cabeçalho IP original;

b) **Modo túnel**: encapsula todo o pacote IP original em um novo cabeçalho IP, criando um túnel seguro entre os pontos de comunicação, muito usado em VPNs.

A Figura 2.8 ilustra essas diferenças. Nos subgráficos (a) e (b), observa-se a utilização do ESP: no modo transporte (a), apenas a carga útil é criptografada, enquanto no modo túnel (b) o pacote inteiro é protegido, incluindo o cabeçalho IP original. Já nos subgráficos (c) e (d), o protocolo AH é empregado: no modo transporte (c), a autenticação e integridade são aplicadas somente à carga, enquanto no modo túnel (d) o pacote completo recebe essa proteção. A principal distinção é que somente o ESP provê confidencialidade, além da autenticação.

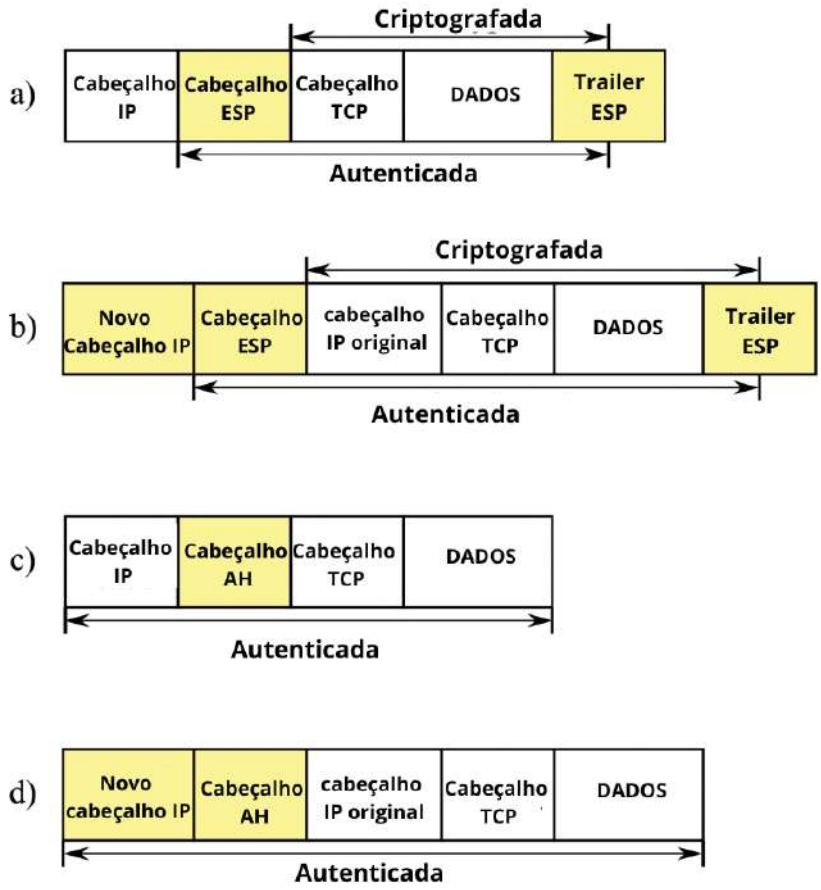



**Figura 2.8:** *Estrutura de pacotes protegidos pelo IPsec: (a) ESP em modo transporte, (b) ESP em modo túnel, (c) AH em modo transporte e (d) AH em modo túnel. Fonte: Adaptado de Quantum Cryptography in 5G Network [Mehic* et al. *2024].*

O conceito central que viabiliza essa proteção é a Associação Segura (*Security Association* – SA). Uma SA é um acordo entre pares de comunicação que define quais protocolos de segurança serão utilizados (ESP ou AH), quais algoritmos criptográficos serão empregados e quais chaves criptográficas serão aplicadas. Cada SA é identificada de forma única pelo *Security Parameter Index* (SPI), transmitido junto a cada pacote no cabeçalho ESP ou AH, combinado ao endereço de destino e ao protocolo IPsec correspondente.

A criação e gerenciamento das SAs são realizados pelo protocolo *Internet Key Exchange* (IKE), que estabelece parâmetros de segurança dinamicamente. Quando criada, cada SA possui um tempo de vida associado, medido em segundos ou em quantidade de bytes processados. Ao expirar, é substituída por outra SA com parâmetros semelhantes, mas novas chaves criptográficas, em um processo denominado *rekeying*. Esse procedimento é essencial, pois o uso prolongado da mesma chave pode facilitar ataques de criptoanálise [Mehic *et al.* 2024].

O IKE é baseado no *Internet Security Association and Key Management Protocol* (ISAKMP) (Maughan et al., 1998, apud [Mehic *et al.* 2024]), e possui duas versões padronizadas: IKEv1 (Harkins, 1998, apud [Mehic *et al.* 2024]) e IKEv2 (Kaufman, 2005, apud [Mehic *et al.* 2024]). O estabelecimento de uma SA IPsec ocorre em duas fases:

a) **Primeira fase:** O IKE autentica os pares, realiza a troca de chaves utilizando o algoritmo Diffie-Hellman (DH) e negocia os parâmetros para uma SA IKE. A partir de segredos derivados (SKEYID ou SKEYSEED, conforme a versão), são geradas as chaves de criptografia e autenticação usadas na comunicação.

b) **Segunda fase:** O canal seguro estabelecido na fase anterior é usado para negociar SAs em nome do IPsec. As chaves de sessão para ESP ou AH são derivadas do segredo estabelecido na fase 1. Caso seja exigida *Perfect Forward Secrecy* (PFS), uma nova troca de chaves DH é realizada. Nesta fase também ocorre a renegociação de chaves (rekeying).

A Figura 2.9 apresenta de forma simplificada o processo de verificação e negociação do IPsec. O fluxo mostra que, para cada pacote, o sistema operacional decide se deve aplicar proteção. Se houver uma SA válida, os serviços de segurança são aplicados; caso contrário, inicia-se a negociação via IKE até que a SA seja estabelecida e o tráfego protegido.

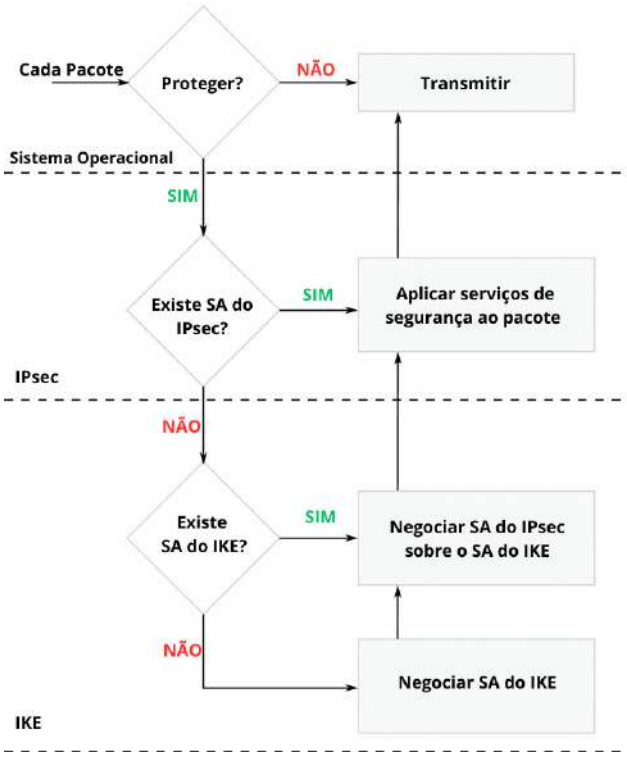



**Figura 2.9:** *Fluxo simplificado de processamento do IPsec e negociação via IKE. Fonte: Adaptado de Quantum Cryptography in 5G Network [Mehic* et al. *2024].*

### Integração de QKD e IPsec

O IPsec oferece segurança limitada porque depende do algoritmo *Diffie–Hellman* (DH), que é apenas computacionalmente seguro. Em cenários de recodificação rápida, o uso de DH pode aumentar a carga da rede e reduzir a taxa de transferência em conexões VPN [Mehic *et al.* 2024]. Essas limitações podem ser superadas com o uso de tecnologias quânticas. Uma visão geral das abordagens atuais de integração entre *QKD* e IPsec é apresentada por Dervisevic e

Mehic (2021, apud [Mehic *et al.* 2024]). Essa integração é necessária porque infraestruturas críticas que dependem do IPsec exigem soluções seguras a longo prazo.

A primeira rede quântica do mundo, a rede DARPA (Elliott et al., 2003; Elliott & Yeh, 2007, apud [Mehic *et al.* 2024]), introduziu VPNs baseadas em IPsec habilitadas para *QKD*. Nesse caso, o caminho de processamento do IPsec e o protocolo IKE foram modificados para usar chaves quânticas com extensões de *reseeding* rápido e com OTP. Na extensão de *reseeding* rápido, chaves de sessão são derivadas de chaves quânticas e usadas em conjunto com cifras simétricas convencionais. As SAs IPsec são recodificadas aproximadamente uma vez por minuto, garantindo renovação periódica das chaves. Já a extensão OTP garante confidencialidade total, aplicando a chave quântica como máscara única de criptografia. A Figura 2.10 apresenta uma visão esquemática dessa integração.

Na Figura 2.10, observa-se que os módulos QKD (à esquerda e à direita) geram conjuntos de chaves quânticas, que são armazenadas e disponibilizadas para o protocolo IKE. Este, por sua vez, combina chaves quânticas com chaves clássicas para formar associações seguras (SAs) do IPsec. Cada SA resultante é utilizada no túnel VPN, proporcionando maior entropia e resiliência contra ataques de criptoanálise.

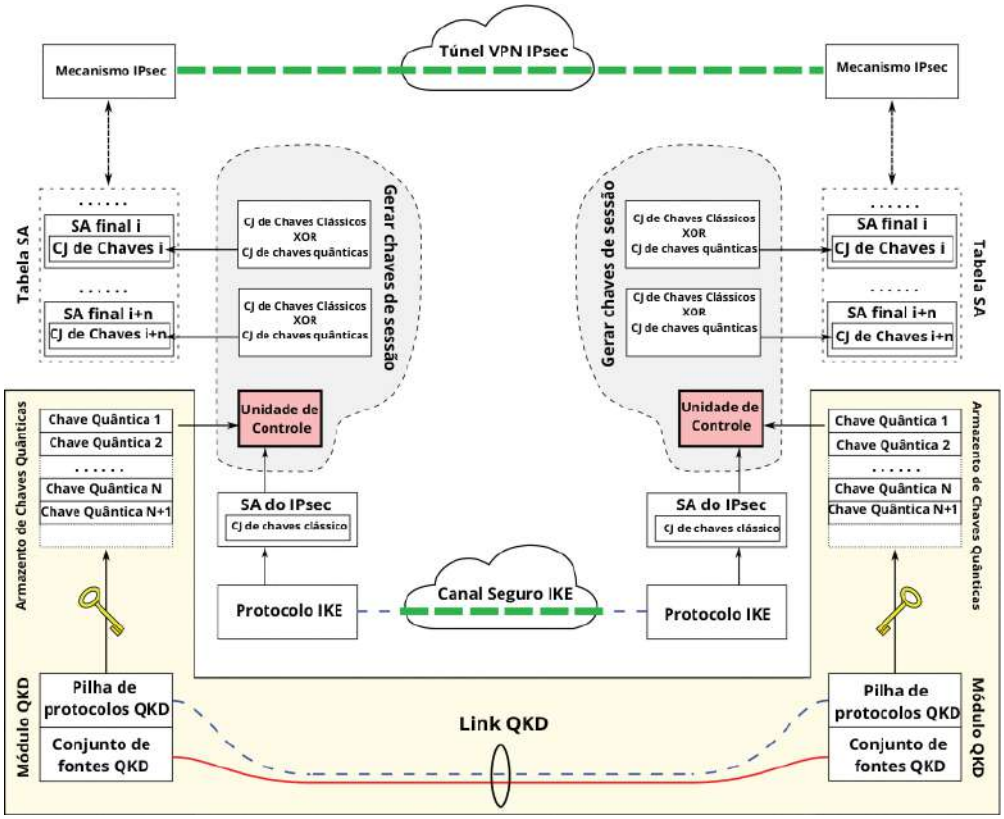



**Figura 2.10:** *Integração de QKD e IPsec: múltiplas SAs são estabelecidas combinando chaves quânticas com chaves clássicas derivadas do IKE. Fonte: Adaptado de Quantum Cryptography in 5G Network [Mehic* et al. *2024].*

Devido a questões de compatibilidade entre IKE e QKD, mencionadas por Elliott et al. (2003, apud [Mehic *et al.* 2024]), foi proposto o protocolo *Secure Quantum Key Exchange Internet Protocol* (SeQKEIP) no projeto SECOQC (Sfaxi et al., 2005, apud [Mehic *et al.*

2024]), criando a primeira rede quântica europeia (Peev, 2009, apud [Mehic *et al.* 2024]). O SeQKEIP introduz uma fase adicional (fase zero), na qual as chaves quânticas são geradas sob demanda pelos protocolos QKD e utilizadas já na autenticação da fase um. Dessa forma, elimina-se a necessidade de grupos DH ou certificados digitais. Essa solução aumenta a segurança, mas pode afetar o desempenho, já que a geração sob demanda de chaves quânticas pode introduzir atrasos.

Outra proposta é o *Quantum Internet Key Exchange* (QIKE),apresentado por Neppach (2008, apud [Mehic *et al.* 2024]), que adapta o IKE clássico para reduzir sobrecarga de comunicação e permitir recodificação frequente. O QIKE mantém duas fases semelhantes ao IKEv1, mas negocia parâmetros adicionais, como taxa de chaves e número máximo de SAs, permitindo coexistência de múltiplas sessões seguras em implementações de alta velocidade. Diferente do IKE clássico, o QIKE não renegocia SAs expiradas: apenas remove as antigas e instala novas localmente com novos SPIs e chaves vindas do gerenciador.

Uma solução simples foi apresentada em Berzanskis et al. (2009, apud [Mehic *et al.* 2024]), que mantém até $2^{16}$ SAs IPsec ativas em cada direção. Essa abordagem gera várias SAs na fase dois do IKE combinando chaves quânticas e clássicas via operação XOR. O benefício dessa técnica é que as chaves finais possuem entropia maior ou igual à das chaves clássicas, aumentando a segurança sem alterar a fase um do IKE.

Mais recentemente, Nagayama e Van Meter (2009, 2014, apud [Mehic *et al.* 2024]), propuseram uma versão modificada do IKEv2, permitindo negociar chaves quânticas já nas trocas iniciais. Foram introduzidas cargas úteis adicionais, como o *KeyID QKD*, que transmite identificadores das chaves e dispositivos QKD. Esse método define ainda estratégias de fallback (*WAIT_ QKD*, *CONTINUE* ou *DIFFIE–HELLMAN*) para garantir continuidade da comunicação caso não haja chaves quânticas disponíveis. Embora eficiente, essa proposta não é adequada a ambientes de altíssima velocidade.

Por fim, Marksteiner e Maurhart (2015, apud [Mehic *et al.* 2024]) apresentaram um protocolo leve de sincronização chamado de *re-chaveamento rápido*, que utiliza um canal de controle autenticado por AH e um canal de dados criptografado por ESP. O protocolo adota a estrutura mestre/escravo: o nó mestre mantém filas de SPIs e chaves quânticas, ativando um par por vez, e notifica o escravo sobre cada mudança de chave. Esse procedimento é ilustrado na Figura 2.11.

Na Figura 2.11, vê-se como o mestre e o escravo mantêm filas paralelas de chaves e SPIs. O elemento ativo (em azul) é usado para cifrar e autenticar pacotes, enquanto novos pares são adicionados e antigos removidos periodicamente. Esse mecanismo permite realizar dezenas de trocas de chave por segundo, garantindo segurança contínua mesmo em conexões de alta velocidade.

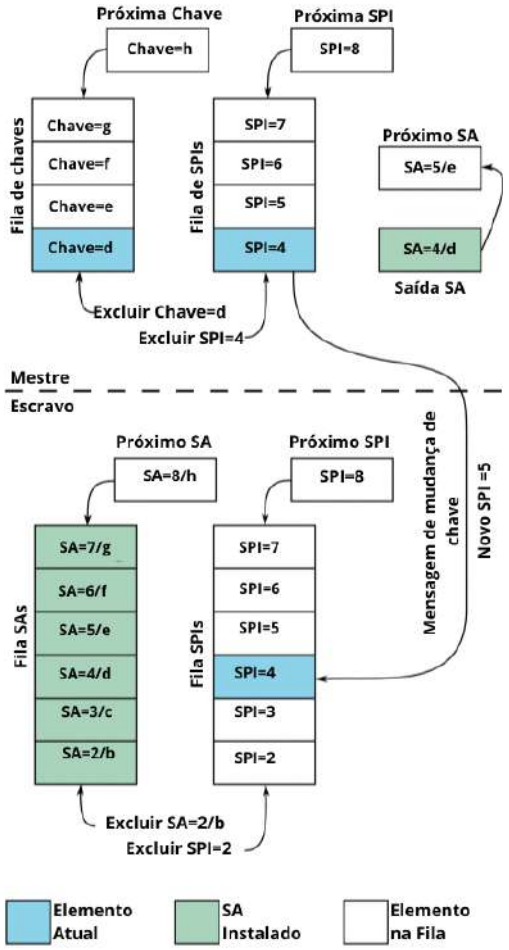



**Figura 2.11:** *Funcionamento do protocolo de re-chaveamento rápido em IPsec com QKD, baseado em filas de chaves e SPIs sincronizados entre mestre e escravo. Fonte: Adaptado de Quantum Cryptography in 5G Network [Mehic* et al. *2024].*

### Segurança de controle de acesso à mídia (*MACsec*)

O IPsec tem sido, há muito tempo, uma solução essencial de criptografia para proteger o tráfego entre locais remotos e filiais, sendo a opção preferida da maioria dos clientes de VPN. Ele é considerado adaptável, independente do meio de transporte e escalável para milhares de dispositivos finais. No entanto, o IPsec começa a apresentar limitações em termos de taxa de transferência total para aplicações mais recentes e provedores de nuvem [Mehic *et al.* 2024].

A computação em nuvem e as novas aplicações mudaram os padrões de tráfego das redes roteadas, superando as taxas de criptografia que o IPsec tradicional consegue oferecer. Estudos demonstram que, ao aplicar criptografia IPsec, o desempenho não acompanha as velocidades de conexão quando as taxas de link chegam a 40/100 Gbps ou mais [Mehic *et al.* 2024]. Além disso, protocolos de segurança que aumentam a sobrecarga e a latência podem afetar negativamente o desempenho das aplicações. Quando é necessário criptografar todo o tráfego que passa pelo roteador, a taxa de transferência fica limitada à capacidade de processamento do mecanismo IPsec, que geralmente representa apenas uma fração da

capacidade total de encaminhamento do roteador.

Para reduzir a dependência do *hardware* criptográfico desses dispositivos, as redes QKD podem usar equipamentos dedicados chamados *QKD encryptors*. As abordagens para implementar esses dispositivos são discutidas na Seção 2.4.

O MACsec, também conhecido como *LinkSec*, é uma solução projetada para fornecer comunicação direta e segura de alta velocidade, baseada no formato de quadro *Ethernet*. Ele funciona bidirecionalmente nas taxas de porta *Ethernet*, independentemente do tamanho do pacote. Como opera na camada 2, o MACsec não apenas protege tráfego IP, mas também protocolos como ARP, descoberta de vizinhos e DHCP.

Diferente do IPsec, que normalmente é implementado em um Circuito Integrado de Aplicação Específica (*Application-Specific Integrated Circuit* - ASIC) centralizado para aceleração criptográfica, o MACsec funciona por porta sem perda de desempenho. Ele adiciona um cabeçalho de Etiqueta de Segurança (*Security Tag* - SecTAG) de 16 bytes e um cabeçalho de Valor de Verificação de Integridade (*Integrity Check Value* - ICV) de 16 bytes. Conforme mostrado na Figura 2.12, os endereços MAC de origem e destino permanecem inalterados. O SecTAG inclui um identificador de protocolo, a versão do MACsec, o comprimento dos dados criptografados, um Número de Pacote (*package number* - PN) para proteção contra ataques de repetição e um Identificador de Canal Seguro (*Secure Channel Identifier* - SCI) para identificar a Associação de Conectividade (CA).

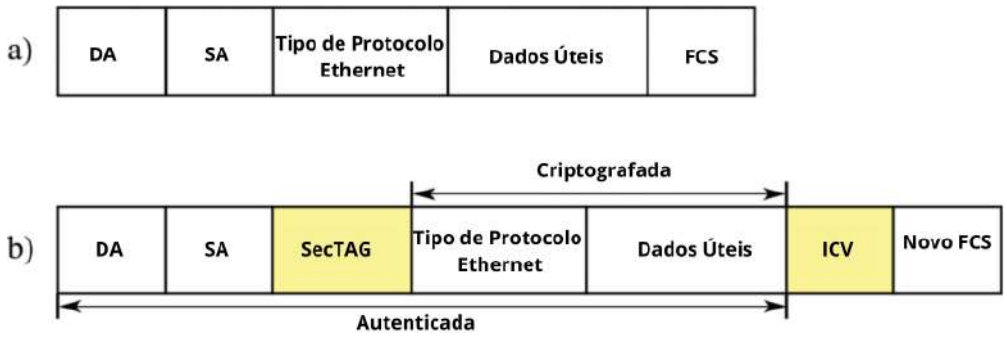



**Figura 2.12:** *a) Formato de quadro Ethernet; b) Formato de quadro MACsec. Fonte: Adaptado de Quantum Cryptography in 5G Network [Mehic* et al. *2024].*

Para garantir a privacidade e a integridade, o quadro MACsec é criptografado e autenticado. Para criptografia autenticada, o MACsec usa o AES-GCM (*Advanced Encryption Standard – Galois/Counter Mode*); para autenticação sem criptografia, utiliza o GMAC (*Galois Message Authentication Code*). Como mostrado na Figura 2.12, o conteúdo criptografado entre os cabeçalhos SecTAG e ICV pode dificultar a leitura por dispositivos intermediários, pois campos como rótulos MPLS, QoS 802.1P e VLAN 802.1Q ficam ocultos.

Apesar dessas limitações, a aplicação ponto a ponto do MACsec combina bem com o conceito de QKD. Como as redes QKD também são baseadas em transporte salto a salto [Mehic *et al.* 2024], a integração dessas duas tecnologias é naturalmente compatível.

**Integrando QKD e MACsec**

A especificação do MACsec não define procedimentos próprios para troca de chaves ou autenticação mútua. Esses procedimentos são realizados por meio de um protocolo complementar conhecido como *MACsec Key Agreement* (MKA), descrito no padrão IEEE 802.1X. O objetivo do MKA é localizar pares MACsec e negociar as chaves de segurança necessárias para proteger o link. Além disso, o MKA também realiza a autenticação e a autorização dos dispositivos conectados à rede. Cada par deve possuir uma chave raiz na hierarquia do MKA, chamada de *Master Session Key* (MSK). A partir dessa MSK são derivadas a *Connectivity Association Key* (CAK) e outras chaves, como a *Integrity Check Key* (ICK), a *Key Encryption Key* (KEK) e a *Secure Association Key* (SAK).

Uma abordagem para integrar QKD e MACsec em redes *Ethernet* seguras foi relatada recentemente em Cho e Sergeev (2021, apud [Mehic *et al.* 2024]). Os autores consideraram diferentes métodos de geração de material de chave, sendo o mais simples utilizar uma chave QKD como uma MSK de 512 bits, a partir da qual a CAK raiz e as demais chaves são derivadas hierarquicamente. Com isso, não são necessárias alterações na estrutura de chaves do MACsec.

Normalmente, usa-se o protocolo EAP para estabelecer a MSK e, a partir dela, derivar hierarquicamente as demais chaves. No entanto, o EAP depende de criptografia de chave pública clássica, vulnerável a ataques quânticos. Por isso, os autores descreveram também a possibilidade de gerar um SAK de sessão de forma independente, executando um protocolo de troca de chaves efêmeras para cada sessão. Assim, se um SAK de sessão for comprometido, os demais permanecem protegidos. Nesse método, as chaves QKD podem ser combinadas com chaves DH de 256 bits para gerar o SAK. Considerando que o *SecTAG* do MACsec possui um campo de Número de Pacotes (PN) de 32 ou 64 bits, uma única chave é suficiente para proteger até $2^{75,6}$ bytes de dados.

Independentemente da abordagem usada para integrar as chaves QKD, a sincronização por meio de identificadores de chave (*KeyID*) é essencial. Os diferentes padrões discutidos na Seção 2.5 podem ser aplicados para buscar e gerenciar as chaves. Vale destacar que, como a QKD é apenas um método de distribuição de chaves, ela não fornece autenticação dos pares MACsec. Tendo abordado as integrações teóricas entre QKD e IPsec/MACsec, a próxima seção discute o desempenho prático de criptografadores de *hardware* que realizam essas operações criptográficas.

## 2.4 Criptografadores QKD

Mudanças na arquitetura de rede e a necessidade de maior densificação levaram ao crescimento do uso da transmissão *fronthaul* no cenário complexo exigido pelas redes 5G. O *fronthaul* óptico corresponde a uma conexão óptica de alta taxa de transferência e baixa latência entre o RRH e a BBU.

A especificação do eCPRI define uma nova interface padrão para redes *fronthaul* ópticas baseadas em *Ethernet*: *"Se a rede de transporte não for segura para um fluxo específico, então um sistema de segurança ponta a ponta da rede eCPRI deve ser implementado no nó eREC e no nó para esse fluxo"* Ericsson (2019, apud [Mehic *et al.* 2024]).

Em outras palavras, para garantir a segurança geral da rede 5G, é fundamental um mecanismo de proteção adequado entre o RRH e a BBU. O protocolo de segurança de rede eCPRI inclui opções como tráfego IPsec (para IP) e MACsec (para *Ethernet*). No entanto, quando IPsec ou MACsec são habilitados, espera-se um aumento de atrasos ou degradação do desempenho no *fronthaul*. A ativação desses protocolos de segurança introduz sobrecarga e tempo adicional de processamento; portanto, é necessária uma avaliação detalhada do impacto no desempenho do *fronthaul* óptico e no transporte de dados em redes 5G.

### 2.4.1 Requisitos para *Fronthaul* 5G

Cho et al [Cho, Sergeev e Zou 2019], avaliaram e analisaram o efeito dos protocolos de segurança no desempenho do *fronthaul* 5G. Os autores pesquisaram soluções de segurança para redes *fronthaul* ópticas baseadas em *Ethernet* e examinaram protocolos de segurança comuns, como IPsec e MACsec. Embora a sobrecarga extra desses protocolos não tenha efeito significativo sobre a latência, os processos de criptografia e descriptografia dos pacotes de transmissão podem impor atrasos adicionais no tempo de processamento do eCPRI e, eventualmente, restringir a distância máxima de transmissão entre a BBU e o RRH.

Foi confirmado experimentalmente que os atrasos adicionais causados pelos procedimentos de criptografia e descriptografia são consideráveis e podem exceder o requisito máximo de latência unidirecional do *fronthaul* (cerca de 100 $\mu$s). A configuração de teste utilizada pelos autores consistia em um gerador de tráfego e dois elementos de rede conectados por uma fibra de 10 GbE. Os resultados foram obtidos a partir de uma implementação de *software* não otimizada; a velocidade poderia ser aumentada por meio da implementação de um criptoacelerador de *hardware*.

Os autores indicaram que a próxima etapa seria examinar uma implementação em FPGA de protocolos de tunelamento seguro (selecionados) que poderiam acelerar o processo de criptografia e descriptografia. Em Carnevale et al. (2017, apud [Mehic *et al.* 2024]), foi proposta uma implementação de *hardware* do MACsec adequada para velocidades de *Ethernet* de até 10 Gbps, introduzindo um atraso inferior a 350 ns. O núcleo de rede AES-GCM foi implementado em um microcontrolador, e os autores indicaram sua possível implementação em FPGA. Embora projetada principalmente para garantir a segurança de *backbones Ethernet* automotivos, a solução relatada pode ser utilizada como parte do protocolo de segurança de rede eCPRI quando o desempenho de rede de 10 Gbps for suficiente.

Considerando o exposto, e o fato de que algoritmos criptográficos frequentemente representam gargalos em toda a cadeia de comunicação, as tarefas de segurança estão sendo cada vez mais transferidas para placas de rede FPGA. Com um FPGA, é possível obter

um aumento significativo na taxa de transferência, além de facilitar a troca de uma operação criptográfica para outra. Como resultado, algoritmos criptográficos e os protocolos MACsec/IPsec são candidatos ideais para implementação em FPGA.

### 2.4.2 Criptografadores baseados em FPGA

Vários trabalhos na literatura apresentam implementações de criptografia de dados baseadas em FPGA; entretanto, poucos abordam de forma completa o funcionamento do MACsec ou do IPsec (ou mesmo de seus principais componentes). Diferentemente desses, o artigo base desta pesquisa tem como foco justamente a integração com os protocolos MACsec e IPsec, além de utilizar FPGA como plataforma de implementação. Por esse motivo, ele foi adotado como referência principal para o desenvolvimento deste trabalho.

Durante a revisão das propostas existentes, observou-se que as soluções de criptografia baseadas em FPGA podem ser organizadas em três modelos principais de arquitetura para criptografadores:

a) **CPU com aceleração de *hardware* baseada em FPGA** (Fig. 2.13);

b) **Arquitetura FPGA autônoma** (Fig. 2.14);

c) **Arquitetura híbrida CPU/FPGA**, ou seja, um projeto combinado de *hardware* e *software* (Fig. 2.15).

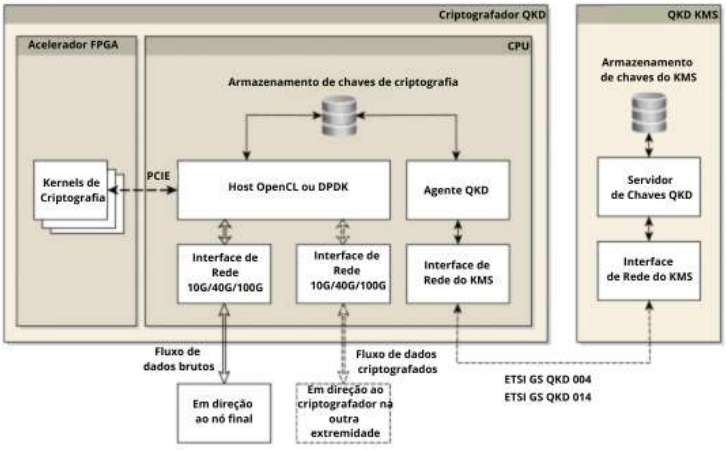



**Figura 2.13:** *Modelo arquitetônico de um criptografador baseado em CPU com aceleração baseada em FPGA. Fonte: Adaptado de Quantum Cryptography in 5G Network [Mehic* et al. *2024].*

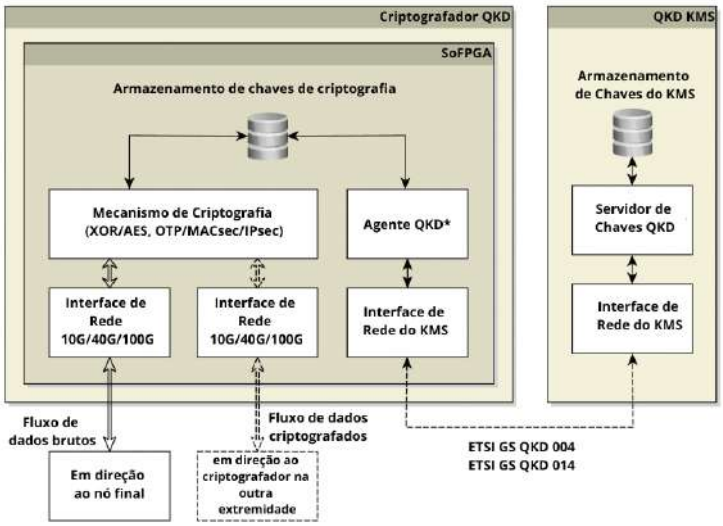



**Figura 2.14:** *Modelo arquitetônico de um criptografador autônomo baseado em FPGA. Fonte: Adaptado de Quantum Cryptography in 5G Network [Mehic* et al. *2024].*

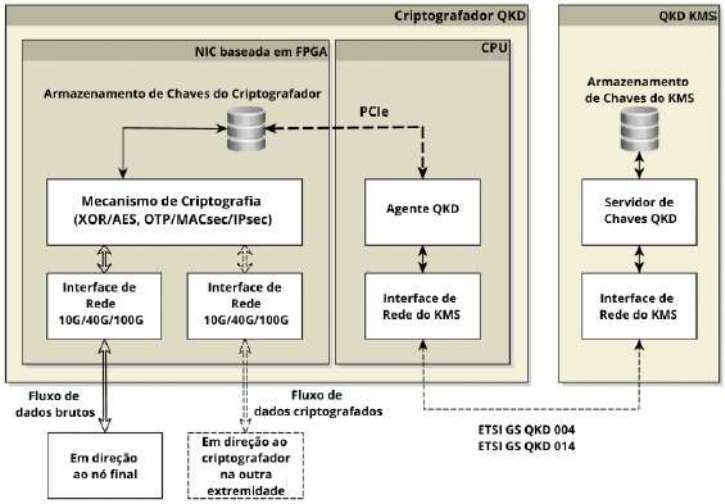



**Figura 2.15:** *Modelo arquitetônico de um criptografador híbrido CPU/FPGA. Fonte: Adaptado de Quantum Cryptography in 5G Network [Mehic* et al. *2024].*

Diversos trabalhos propuseram implementações do IPsec em FPGA para reduzir a carga computacional e aumentar o desempenho em redes de alta velocidade. Rao et al. (2018, apud [Mehic *et al.* 2024]) apresentaram um núcleo IPsec baseado em FPGA, suportando modos de transporte e túnel com os protocolos AH e ESP, utilizando algoritmos como SHA-3 e AES. Testes em dispositivos *Xilinx Virtex-5* e *Virtex-6* estimaram taxas na ordem de Gbps para datagramas IPv4 de 576 bytes. Driessen et al. (2012, apud [Mehic *et al.* 2024]) também demonstraram síntese de núcleos IPsec para a família Spartan, destacando potencial prático em diferentes modelos de arquiteturas.

Vajaranta et al. (2018, apud [Mehic *et al.* 2024]) avaliaram um acelerador IPsec em FPGA integrado a um conceito SDN, atingindo 1,4 Gbps com pacotes de 64 bytes em um *Arria 10 GX1150*. Já Salman (2011, apud [Mehic *et al.* 2024]) propôs uma abordagem baseada em

reconfiguração parcial para dispositivos limitados, alcançando cerca de 650 Mbps, embora o processo de reconfiguração ainda seja um gargalo.

Lu e Lockwood (2005, apud [Mehic *et al.* 2024]) apresentaram uma solução híbrida CPU/FPGA com IPsec em modo transporte, obtendo 1,2 Gbps com AES e HMAC. Nguyen et al. (2018, apud [Mehic *et al.* 2024]) propuseram arquitetura multicore com *pipeline*, atingindo 2,36 Gbps. Korona et al. (2017, apud [Mehic *et al.* 2024]) implementaram um gateway IPsec autônomo em um *Stratix V*, atingindo até 10 Gbps com DES e 5,5 Gbps com AES, demonstrando ganhos significativos com paralelismo. Martinasek et al. (2018, apud [Mehic *et al.* 2024]) propuseram arquitetura AES-GCM altamente paralela, atingindo 200 Gbps em uma placa *Xilinx Virtex UltraScale+* com oito módulos AES-GCM.

Para o MACsec, Govindan et al. (2019, apud [Mehic *et al.* 2024]) implementaram um *switch Ethernet* habilitado para MACsec em uma placa *NetFPGA-SUME* (Virtex-7), usando uma arquitetura híbrida CPU/FPGA. Embora sem dados detalhados de desempenho, demonstraram a viabilidade de integrar módulos MACsec ao *pipeline* de rede. Uma visão geral dessas soluções testadas em *hardware* encontra-se resumida na Tabela 2.2.

| Reference | FPGA Platform | Protocol | Algorithms | Clock freq. (MHz) | Packet size (bytes) | Throughput (Gbps) |
|---|---|---|---|---|---|---|
| Korona et al. [142] | Intel Stratix V | IPsec | DES, HMAC-SHA1 | 100.65 | 1500 | 10.227 |
| Korona et al. [142] | Intel Stratix V | IPsec | AES, HMAC-SHA1 | 97.98 | 1500 | 5.518 |
| Martinasek et al. [143] | Xilinx Virtex UltraScale+ | IPsec | AES-GCM | 200 | *not specified* | 200 |
| Lu and Lockwood [140] | Xilinx Virtex-II Pro | IPsec | AES-CBC, HMAC-MD5/SHA1 | 196.3 | *not specified* | *1.2* |
| Nguyen et al. [141] | Xilinx Virtex-6 | IPsec | AES-CBC/GCM, HMAC-SHA5 | 100 | *1500* | *2.36* |

**Tabela 2.2:** *Tabela comparativa de implementações de IPsec baseadas em FPGA. Fonte: Adaptado de Quantum Cryptography in 5G Network [Mehic* et al. *2024].*

Observa-se que implementações altamente paralelas de algoritmos de criptografia oferecem o melhor desempenho de *throughput*, chegando a 200 Gbps em protótipos e até 482 Gbps em um único FPGA Xilinx Virtex Ultrascale, com possibilidade de superar 800 Gbps em configurações com múltiplos FPGAs. Vale ressaltar que a maioria dos estudos não considerou o impacto do intervalo de renovação de chaves no desempenho do sistema.

Arquiteturas FPGA autônomas, como a descrita em Lorunser (2008, apud [Mehic *et al.* 2024]), integram módulos de comunicação clássica em *software* e interfaces de pré-processamento e IPsec em *hardware*, demonstrando viabilidade, embora sem dados de latência. Já arquiteturas híbridas CPU/FPGA, como a proposta em Muehlberghuber et al. (2012, apud [Mehic *et al.* 2024]), combinam subsistemas FPGA e *QKD* e atingiram taxas de até 133 Gbps.

Além disso, criptografadores comerciais habilitados para *quantum*, como as séries *Centauris CN6000* e *CN9000* da *ID Quantique* (até 100 Gbps) e o *FSP 150-XG118Pro* da *ADVA*, mostram que FPGAs são ideais para a fase atual de integração entre 5G e QKD, oferecendo flexibilidade, atualizações em campo e tempos reduzidos de lançamento. No futuro, espera-se

a migração para ASICs, proporcionando maior eficiência energética e desempenho superior.

## 2.5 Padrões *QKD*

A integração da tecnologia *QKD* em redes IP exige padronização para garantir interoperabilidade e segurança. Nos últimos anos, diversas organizações internacionais têm desenvolvido normas e diretrizes para viabilizar o uso de *QKD* em grande escala.

O IEEE estabeleceu em 2016 o padrão IEEE-SA P1913, que define especificações para bits quânticos, sem considerar inicialmente seu uso prático (IEEE, 2016, apud [Mehic *et al.* 2024]). A ITU-T apoiou projetos nos grupos de estudo SG13 (ITU-T, 2020, apud [Mehic *et al.* 2024]) e SG17 (ITU-T, 2020, apud [Mehic *et al.* 2024]) para investigar arquiteturas e modelos de organização de redes *QKD*. Em 2019, foi criado o FG-QIT4N, focado em tecnologias quânticas para redes. O IETF formou o grupo de pesquisa QIRG para explorar protocolos baseados em emaranhamento quântico, buscando superar limitações de distância. Já a ISO criou o comitê ISO/IEC JTC 1/SC 27 para especificação, avaliação e testes de soluções *QKD* (ISO, 1989, apud [Mehic *et al.* 2024]). Além disso, o ETSI mantém um grupo de trabalho dedicado à criptografia quântica segura, integrando esforços da academia e da indústria (ETSI, 2022, apud [Mehic *et al.* 2024]).

Entre os padrões mais relevantes destacam-se o ETSI GS *QKD* 004 e o ETSI GS *QKD* 014, que definem uma API entre aplicativos e componentes de rede *QKD*. Esses padrões assumem que a rede *QKD* é organizada em zonas de domínio restrito, com o KMS como elemento central responsável pela entrega de chaves. Por exemplo, quando o aplicativo SAE de Alice deseja se comunicar com o SAE de Bob, envia uma mensagem *OPEN_CONNECT* ao KMS mais próximo, reservando chaves em ambos os lados e garantindo critérios mínimos de QoS antes de estabelecer a conexão.

A Figura 2.16 apresenta o diagrama de sequência da interface de aplicação definida pelo padrão ETSI 004. Ela ilustra como os aplicativos se comunicam com KMS para reservar chaves quânticas e garantir requisitos mínimos de qualidade de serviço (QoS). Observa-se o envio da mensagem *OPEN_CONNECT* do aplicativo de Alice para o KMS, a validação e a reserva de chaves, e a confirmação de disponibilidade antes de estabelecer a conexão segura com o aplicativo de Bob. O diagrama evidencia a centralidade do KMS na coordenação das chaves, refletindo a abordagem do ETSI 004 em manter um controle rigoroso sobre a alocação de recursos criptográficos.

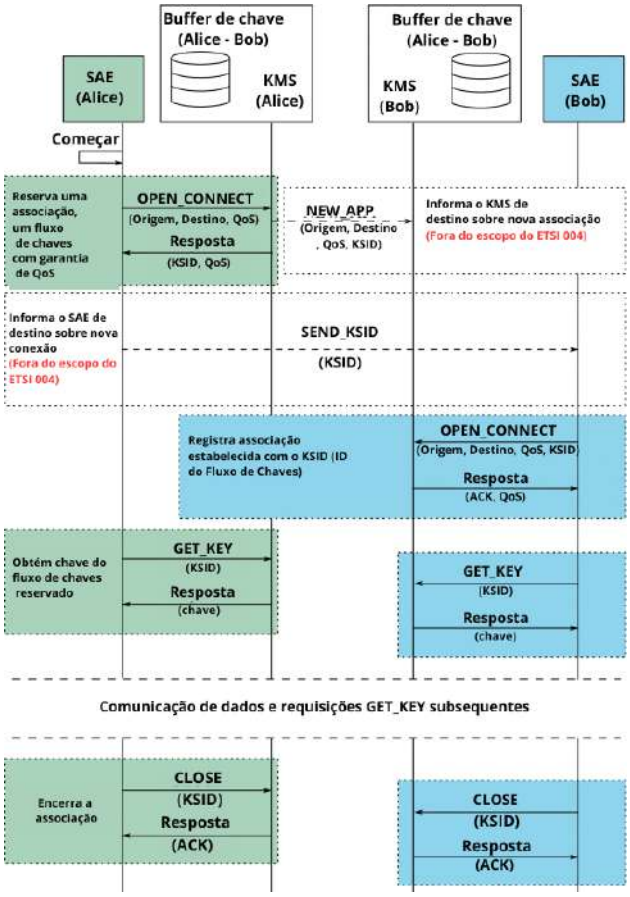



**Figura 2.16:** *Diagrama de sequência da interface de aplicação ETSI 004 trocando especificações de QoS . Fonte: Adaptado de Quantum Cryptography in 5G Network [Mehic* et al. *2024].*

A Figura 2.17 mostra o diagrama de sequência do padrão ETSI 014, que define o protocolo e o formato de dados da interface de programadores de aplicativos (API REST) para entrega de chaves quânticas. Diferentemente do ETSI 004, neste padrão o aplicativo realiza consultas *GET_STATUS* e *GET_KEY* diretamente, assumindo parte da responsabilidade pela verificação da disponibilidade de chaves. O diagrama evidencia que o KMS atua de forma mais simplificada, sem realizar reservas de longo prazo, refletindo a filosofia do ETSI 014 de descentralizar parte do gerenciamento e permitir maior flexibilidade para aplicativos que necessitam de chaves de forma esporádica.

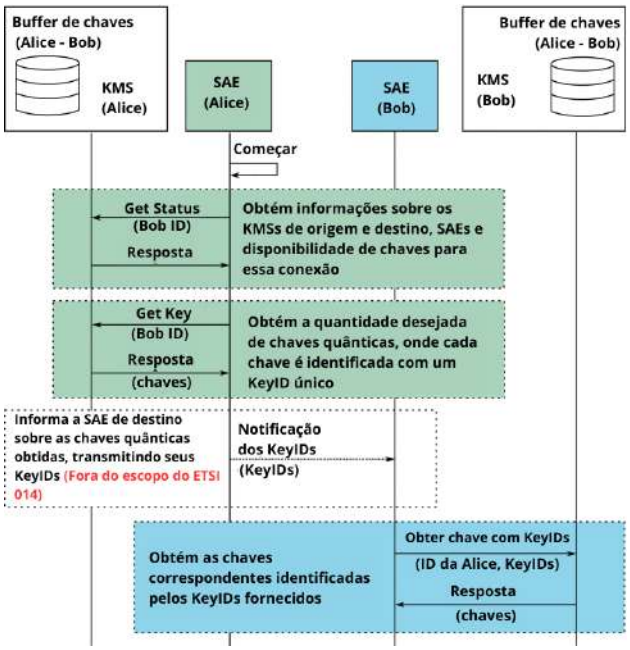



**Figura 2.17:** *Diagrama de sequência do ETSI 014 – Protocolo e formato de dados da interface de programadores de aplicativos de entrega de chaves baseada em REST (API). Fonte: Adaptado de Quantum Cryptography in 5G Network [Mehic* et al. *2024].*

O aplicativo consegue acessar as chaves reservadas enviando consultas *GET_KEY* dedicadas, juntamente com o ID da sessão previamente estabelecida. Observa-se que as chaves na abordagem *QKD* são geradas em blocos com identificadores únicos, sendo que os tamanhos desses blocos podem variar conforme o tipo de dispositivo *QKD*. A comunicação entre os KMS desempenha, portanto, um papel importante na compactação, mesclagem e combinação de blocos de tamanhos diferentes, seja de forma antecipada ou sob demanda. Entretanto, o padrão ETSI 004 não define comunicações de sinalização KMS–KMS ou APP–APP, que seriam críticas para a sincronização das solicitações de reserva e do armazenamento de chaves (buffers).

Ao contrário do padrão ETSI 004, no qual o KMS executa uma função de reserva e possui um papel central na verificação da disponibilidade de chaves *QKD* em um caminho especificado entre aplicativos, o padrão ETSI 014 permite uma implementação mais simples das entidades KMS. Este não possui mecanismos de reserva de longo prazo, e o próprio aplicativo é responsável por consultar o status de disponibilidade do caminho da chave. Ao enviar uma consulta RESTful *GET_STATUS*, o aplicativo solicita informações sobre a disponibilidade do caminho até o hub remoto. Caso a resposta seja satisfatória, o aplicativo pode solicitar uma chave de segurança para um destino remoto, mas não em quantidade superior ao valor definido na resposta à consulta *GET_STATUS*. Assim como no ETSI 004, o padrão ETSI 014 também não define comunicações de sinalização KMS–KMS ou APP–APP.

A diferença principal entre esses dois padrões reflete-se na forma como a funcionalidade de QoS é fornecida. O padrão ETSI 014 é mais adequado para redes com entidades KMS

mais simples e aplicativos que necessitam de chaves apenas ocasionalmente, visto que o envio frequente de mensagens *GET_STATUS* e *GET_KEY* pode gerar sobrecarga nas entidades KMS. Tanto o ETSI 004 quanto o ETSI 014 dependem do protocolo HTTPS para a transmissão de informações de sinalização e de chaves criptográficas.

# Capítulo 3

# Materiais e Métodos

A metodologia adotada neste trabalho é de natureza qualitativa, exploratória e fundamentada em análise bibliográfica. O propósito central é compreender e interpretar, a partir da literatura científica, as contribuições e limitações da criptografia quântica, em especial do protocolo QKD, aplicadas ao contexto das redes 5G.

## 3.1 Abordagem de Pesquisa Qualitativa

A pesquisa qualitativa caracteriza-se por priorizar a análise interpretativa dos fenômenos, buscando compreender significados, padrões e contextos, em vez de mensurar ou quantificar dados. Diferentemente da pesquisa quantitativa, que se apoia em métodos estatísticos e métricas objetivas, a qualitativa busca examinar a complexidade de determinado tema, permitindo uma visão aprofundada e contextualizada do objeto de estudo. De acordo com [Minayo 2012], esse tipo de abordagem é adequada quando se pretende compreender fenômenos complexos que envolvem múltiplas dimensões, como ocorre nas áreas de segurança da informação e tecnologias emergentes.

Nesse sentido, a pesquisa qualitativa foi escolhida porque o estudo sobre criptografia quântica em redes 5G envolve tanto aspectos técnicos (protocolos, integração em infraestruturas de rede, desempenho) quanto conceituais (modelos de segurança, confiabilidade, aplicabilidade em cenários futuros). Esses elementos não podem ser plenamente analisados apenas por métricas quantitativas, sendo necessário um exame crítico e interpretativo da literatura disponível.

## 3.2 Natureza Exploratória da Pesquisa

Além de qualitativa, a pesquisa possui natureza exploratória. Segundo [Gil 2008], a pesquisa exploratória tem como finalidade principal proporcionar maior familiaridade com o problema investigado, de modo a torná-lo mais explícito ou a construir hipóteses para estudos futuros. Ela é recomendada quando o objeto de estudo ainda é recente ou pouco consolidado, como

é o caso da aplicação prática da *QKD* em redes 5G.

A natureza exploratória também se justifica pelo fato de que a integração entre criptografia quântica e infraestruturas de comunicação móveis é um campo emergente, em constante evolução tecnológica e ainda sem padronizações consolidadas. Assim, a pesquisa não busca testar hipóteses experimentais, mas mapear, organizar e discutir criticamente as principais contribuições acadêmicas e técnicas relacionadas ao tema.

## 3.3 Critério de Escolha do Artigo Base

O artigo *Quantum Cryptography in 5G Networks: A Comprehensive Overview* [Mehic *et al.* 2024], publicado em 2024 pela IEEE, foi selecionado como principal referência para este trabalho. A escolha desse artigo se justifica pelos seguintes motivos:

a) Trata-se de uma revisão abrangente e sistemática, que organiza os principais conceitos, protocolos, padrões e aplicações de *QKD* em redes 5G;

b) É um artigo recente, refletindo o estado da arte da pesquisa e das discussões acadêmicas sobre o tema;

c) Foi publicado em um periódico da IEEE, uma das instituições mais reconhecidas internacionalmente em ciência e engenharia, o que assegura rigor metodológico e qualidade científica;

d) O conteúdo foi revisado por pares (*peer-reviewed*), garantindo confiabilidade e validação da comunidade científica;

e) O artigo dialoga com diferentes perspectivas — teóricas, técnicas e aplicadas — permitindo uma análise rica e multifacetada.

Assim, a utilização desse artigo como base garante que o presente trabalho se apoie em uma fonte consolidada, atualizada e academicamente reconhecida.

## 3.4 Procedimentos Metodológicos

A partir do artigo selecionado, foi realizada uma análise temática, método que consiste em identificar, organizar e interpretar os principais eixos temáticos abordados pelo autor. Esses eixos foram sistematizados em categorias como: fundamentos da criptografia quântica, protocolos de *QKD*, desafios técnicos, integração em redes 5G, padrões e aplicações práticas.

Além da análise direta do artigo, outras referências acadêmicas e técnicas foram consultadas, com o objetivo de complementar e confrontar os conceitos apresentados. Esse cruzamento de informações permitiu validar a consistência das ideias centrais e ampliar a compreensão crítica do tema.

Durante a redação, ferramentas de Inteligência Artificial (*Artificial Intelligence* – IA), como o assistente *ChatGPT*, foram utilizadas exclusivamente como apoio para revisão gramatical, organização textual e adequação ao formato acadêmico, sem interferir no processo de análise crítica ou nas escolhas metodológicas do autor.

# Capítulo 4

# Desenvolvimento

O presente capítulo tem como objetivo apresentar e analisar a aplicação prática da Distribuição de Chaves Quânticas (*QKD*) em redes 5G, explorando como essa tecnologia pode ser integrada aos diferentes segmentos da rede para aumentar a segurança das comunicações. Com base nos conceitos teóricos discutidos no capítulo anterior, este capítulo detalha a utilização de *QKD* em cenários reais e simulados, avaliando seu impacto sobre a confidencialidade, integridade e disponibilidade dos dados trafegados.

Serão abordadas estratégias de integração da *QKD* com arquiteturas modernas de redes 5G, incluindo o gerenciamento centralizado via SDN (*Software Defined Networking*) e a virtualização de funções de rede (*Network Function Virtualization – NFV*). Além disso, serão discutidos casos de estudo que evidenciam a implementação prática da *QKD* em fronthaul e backhaul de redes 5G, bem como a interação com mecanismos de segurança clássicos, como VPNs, IPsec e MACsec.

O objetivo principal deste capítulo é demonstrar, de forma estruturada e fundamentada, como a *QKD* contribui para reforçar a segurança em redes 5G, evidenciando suas vantagens, limitações e desafios de implementação prática.

## 4.1 Aplicações de *QKD* em Redes 5G

Esta seção apresenta e analisa as principais aplicações práticas da tecnologia de *QKD* em redes 5G. São abordadas as estratégias de integração da *QKD* aos diferentes segmentos dessas redes, destacando-se componentes como o gerenciamento baseado em SDN e a utilização de NFV. O objetivo é evidenciar como a *QKD* pode complementar e reforçar os mecanismos de segurança existentes, contribuindo para a construção de infraestruturas 5G mais seguras e resilientes frente às ameaças atuais e futuras.

### 4.1.1 Gerenciamento de Redes *QKD*

A Rede Quântica de Madri é atualmente a maior plataforma dedicada à avaliação prática da tecnologia *QKD* em áreas metropolitanas europeias (Martin, 2019; Aguado, 2019, apud

[Mehic *et al.* 2024]). Seu objetivo principal é integrar a *QKD* a sistemas de telecomunicações já existentes, evitando a necessidade de construção de uma infraestrutura exclusivamente quântica.

Em 2018, um grupo de pesquisa formado pela *Huawei Technologies Düsseldorf* (HWDU), pelo Centro de Pesquisa de Munique, pela UPM e pela Telefónica implementou uma rede em topologia de anel com perímetro de aproximadamente 15 km, interligando três nós *QKD* por meio de fibras escuras dedicadas. Conforme relatado em Lopez (2020, apud [Mehic *et al.* 2024]), foram utilizados dispositivos HWDU de Distribuição Contínua de Chaves Quânticas Variáveis (*Continuous Distribution of Variable Quantum Keys* - CV-*QKD*) para fornecer gerenciamento de rede baseado em SDN. Cada nó foi equipado com uma caixa óptica *QKD* 3U e um servidor *Supermicro 1028R* responsável pelas operações de pós-processamento. Nessa configuração, a taxa de geração de chaves alcançou até 3 kbps em um canal com atenuação de 12 dB.

Para a criptografia de dados, foram utilizadas placas *Huawei TNF1LTX* de 10 portas, compatíveis com chaves *QKD* e com suporte ao algoritmo AES. O gerenciamento da rede foi projetado de acordo com práticas e ferramentas comuns a engenheiros de telecomunicações, garantindo maior eficiência na instalação e operação. Dessa forma, a rede é administrada a partir de uma abordagem SDN, permitindo flexibilidade e escalabilidade.

Além disso, conforme descrito em Lopez (2020, apud [Mehic *et al.* 2024]), um controlador SDN externo foi posicionado além do perímetro de segurança, possibilitando o gerenciamento de outros nós que não utilizam *QKD*. A Figura 4.1 ilustra o esquema de comunicação entre o controlador SDN e os agentes SDN localizados em cada nó da rede. Com base nas informações coletadas, uma rota apropriada é calculada e, como o controlador não armazena material de chave, qualquer comprometimento de sua segurança não afeta o material criptográfico estabelecido entre os nós. A partir do caminho calculado, o LKMS (*Local Key Management System*) presente em cada nó pode executar o encaminhamento de chaves no modo de retransmissão.

A Figura 4.1 ilustra o esquema de gerenciamento de nós de uma rede *QKD* baseada em SDN. Cada nó possui agentes SDN que se comunicam com um controlador externo responsável pelo cálculo de rotas e encaminhamento de chaves, sem armazenar material criptográfico. O diagrama evidencia a integração entre o controlador e os nós, permitindo a implementação de políticas de roteamento seguras e flexíveis, enquanto mantém a segurança das chaves quânticas geradas nos nós da rede.

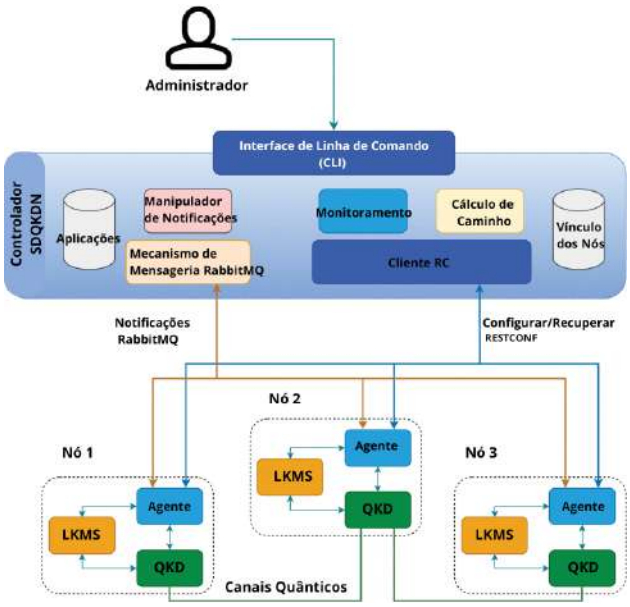



**Figura 4.1:** *Esquema da abordagem de rede SDN no gerenciamento de nós de rede QKD. Fonte: Adaptado de Quantum Cryptography in 5G Network [Mehic* et al. *2024].*

Em Aguado (2018, apud [Mehic *et al.* 2024]), os autores descreveram diversas abordagens para integrar a negociação de chaves *QKD* em infraestruturas de rede baseadas em SDN. Foram propostos fluxos de trabalho potenciais aplicáveis a GMPLS, NETCONF e OpenFlow, utilizados na interface *northbound* de um roteador virtual, atuando como ponto final para comunicações seguras.

Na abordagem centralizada (NETCONF e OpenFlow), as regras de configuração e de encaminhamento são gerenciadas por um controlador responsável pela troca de chaves. Para o estabelecimento de um caminho MPLS, o *Path Computation Element* (PCE) utiliza um *Explicit Route Object* (ERO) modificado em mensagens RSVP, definindo a rota e permitindo a distribuição dos detalhes da chave (ID, comprimento, algoritmo de criptografia, tempo de renovação etc.), bem como demais parâmetros MPLS. O resultado é um caminho MPLS estabelecido com rótulos definidos e informações de chaves *QKD* integradas, conforme ilustrado na Figura 4.2.

A Figura 4.2 apresenta o esquema de sinalização para comunicações com entidades *QKD*. Ela demonstra como informações de configuração e detalhes de chave (ID, comprimento, algoritmo e tempo de renovação) são distribuídos em caminhos MPLS, utilizando protocolos como RSVP, NETCONF ou OpenFlow. O diagrama evidencia o processo de integração da negociação de chaves quânticas com protocolos de controle de rede, garantindo que as comunicações sejam seguras e que o roteamento esteja corretamente configurado para cada sessão.

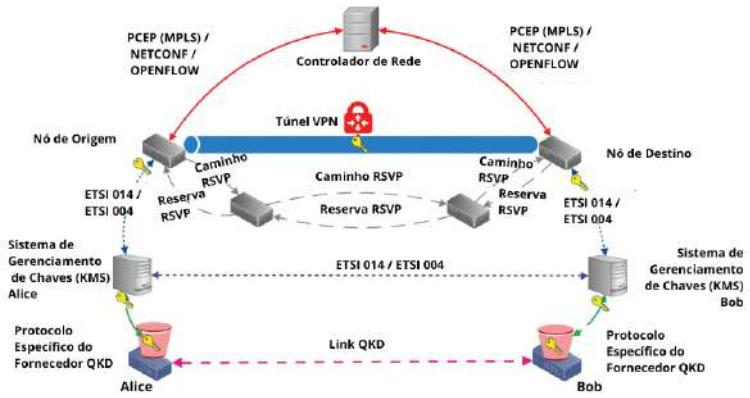



**Figura 4.2:** *Esquema das soluções de sinalização aplicadas às comunicações com entidades QKD. Fonte: Adaptado de Quantum Cryptography in 5G Network [Mehic* et al. *2024].*

Para evitar o uso do protocolo RSVP, pode-se aplicar o NETCONF ou o OpenFlow [Mehic *et al.* 2024]. O NETCONF, sendo baseado em transações, permite reverter automaticamente qualquer configuração incorreta, dispensando a espera por respostas a cada solicitação. Já o OpenFlow exige confirmação explícita do dispositivo, como a verificação de extração de chave ou o estabelecimento dos detalhes de sessão. As propostas dos autores incluem modificações em mensagens OpenFlow, como *Features Reply* e *Flow Mod*, para integração com *QKD*, além do uso de mensagens *Barrier Request/Reply*. Para o NETCONF, foi introduzido um modelo YANG estendido, abrangendo troca de capacidades e sincronização de chaves. Esse modelo foi posteriormente incorporado ao padrão ETSI 015 ETSI (2021, apud [Mehic *et al.* 2024]).

Em Aguado (2017, apud [Mehic *et al.* 2024]), os autores investigaram a utilização de chaves *QKD* para proteger comunicações de gerenciamento de rede em cenários de NFV. Sessões SSH foram estendidas com a biblioteca *Python paramiko*, enquanto a camada SSL/TLS foi implementada usando *tlslite-ng*. Após receber a solicitação para implantar uma infraestrutura virtual, o orquestrador coleta informações sobre a topologia e envia instruções ao controlador SDN ONOS, que estabelece a conectividade entre hosts usando intenções baseadas em MAC. Toda a comunicação ocorre por sessões SSH protegidas por chaves quânticas.

Uma abordagem ampliada foi relatada por Aguado (2017, apud [Mehic *et al.* 2024]), onde o controlador SDN também define e controla conexões ópticas em switches ópticos programáveis (*Polatis*), permitindo o estabelecimento dinâmico de múltiplas conexões seguras entre dispositivos *QKD* remotos e servidores de chaves.

Os autores em Wright (2021, apud [Mehic *et al.* 2024]) demonstraram a *Bristol 5GUK Test Network*, uma rede que aplica fatiamento dinâmico com base em segurança *QKD* e criptografia *quantum-safe*. A infraestrutura usa dispositivos compatíveis com NETCONF e modelos YANG para configuração. Um orquestrador automatizado envia instruções ao controlador, reduzindo significativamente o tempo de configuração do fatiamento de rede.

Por fim, Hugues-Salas (2019, apud [Mehic *et al.* 2024]) apresentou uma abordagem que responde dinamicamente a ataques na camada física da rede. Utilizando um *Quantum Para-*

*meter Monitor* (QPM), parâmetros como a taxa de erro quântico (QBER) e a taxa de chaves são monitorados em tempo real. Caso valores críticos sejam detectados, o QPM instrui o controlador SDN *OpenDaylight* a redirecionar o tráfego por um caminho óptico alternativo. Todas as informações são registradas em um banco de dados *SQLite*, permitindo detecção de anomalias e ajustes rápidos na operação da rede, conforme ilustrado na Figura 4.3.

A Figura 4.3 mostra a abordagem de monitoramento em tempo real de nós de rede *QKD* em uma arquitetura SDN. O diagrama destaca o uso do *Quantum Parameter Monitor* (QPM) para medir parâmetros críticos, como a taxa de erro quântico (QBER) e a taxa de geração de chaves. Caso sejam detectados valores fora do esperado, o controlador SDN redireciona o tráfego por caminhos ópticos alternativos, garantindo continuidade e segurança na operação da rede. O esquema também evidencia o registro das informações em banco de dados para análise de anomalias e ajuste dinâmico da infraestrutura.

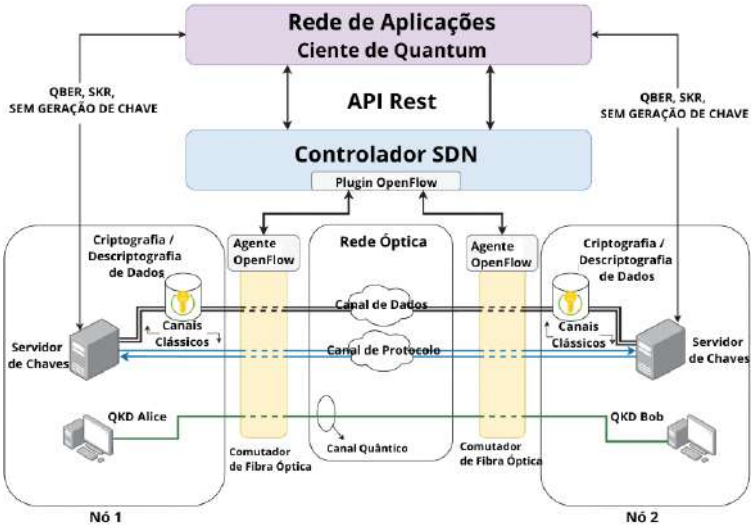



**Figura 4.3:** *Esquema da abordagem de rede SDN para monitoramento em tempo real de nós de rede QKD e gerenciamento de switches de fibra óptica . Fonte: Adaptado de Quantum Cryptography in 5G Network [Mehic* et al. *2024].*

### 4.1.2 *QKD* no Fronthaul 5G

Embora as redes *fronthaul* baseadas em *Ethernet* forneçam transmissão de dados eficiente, elas também apresentam novos desafios. Uma rede *fronthaul* móvel deve atender a requisitos rigorosos de atraso, especialmente para suportar os novos serviços sensíveis a latência introduzidos no 5G. De acordo com a pesquisa apresentada em [Bjømstad, Chen e Veisllari 2018], cumprir esses requisitos de atraso implica restringir a distância de transmissão a menos de 20 km.

Como a rede *fronthaul* móvel 5G transporta grandes volumes de dados agregados dos usuários, ela se torna um alvo potencial para ataques, tornando necessário reforçar a segurança. A especificação eCPRI recomenda o uso de mecanismos como *MACsec* ou IPsec para proteção dos dados. No entanto, esses protocolos introduzem um atraso adicional de

processamento que não pode ser ignorado.

Estudos conduzidos por Cho et al. (2019, apud [Mehic *et al.* 2024]) mostram que a criptografia e a descriptografia unidirecional realizadas por *software* acrescentam um atraso aproximado de 34 $\mu$s, resultando em um limite máximo de distância de transmissão inferior a 17,8 km. Embora essas distâncias reduzidas possam parecer uma limitação, elas favorecem a aplicação de tecnologias como a *QKD*, uma vez que a distribuição de chaves quânticas tende a ser mais eficiente em enlaces de menor extensão.

### 4.1.3 Estudo de Caso 1

A integração de *QKD* em uma rede *fronthaul* móvel 5G óptica baseada em *Ethernet* foi analisada por [Zavitsanos *et al.* 2020]. O desempenho de um sistema BB84-*QKD* de codificação de fase, utilizando dispositivos comerciais da *ID Quantique (Cerberis2* e *id3100 Clavis2*), foi avaliado levando em conta as restrições de latência da rede. Para diferentes níveis de segurança, foram definidas taxas de atualização AES-256 (*re-keying*) de 1,4 s, 1 min e 5 min, correspondendo a taxas de chave segura de 183 bps, 4,3 bps e 0,83 bps, respectivamente.

O estudo considerou duas configurações:

a) Fibra escura: o canal quântico é implementado em um link dedicado, oferecendo maior desempenho.

b) Fibra compartilhada: canais quântico e clássico coexistem na mesma fibra, permitindo reutilizar a infraestrutura existente, mas reduzindo o desempenho devido ao espalhamento Raman. Aumentar a separação espectral entre os canais reduz essa contaminação.

Foram exploradas topologias ponto a ponto (*point to point* - P2P) e Ponto a Multiponto (P2MP). A configuração de fibra compartilhada em topologia P2MP reduziu os custos de implementação, porém com perda significativa de desempenho do canal quântico e aumento do número de nós finais. Na topologia P2MP, um único transmissor quântico atende múltiplos receptores, redirecionando fótons para diferentes destinos por meio de um comutador óptico passivo, distribuindo as chaves entre todos os nós.

Também foi analisada a configuração P2MP *upstream*, onde um único receptor quântico de alta velocidade é compartilhado por vários transmissores. Essa abordagem apresenta vantagens por exigir apenas um detector de fóton único , componente mais caro e sensível, e permitir uma taxa de geração de chaves ajustável por usuário [Mehic *et al.* 2024].

| Topology | P2P | | P2MP | | | | | |
|---|---|---|---|---|---|---|---|---|
| Configuration | Dark fiber | Shared fiber | Dark fiber | | | Shared fiber | | |
| Spectral allocation Quantum channel | C-band | | C-band | | | | | |
| Spectral allocation Classical channels | - | O-band | - | | | O-band | | |
| Number of end nodes for P2MP | - | | 4 | 16 | 64 | 4 | 16 | 64 |
| Distance limit [km] for 183 bps SKR | 17 | 10.5 | 17 | | 8 | 9.5 | 7 | 2 |
| Distance limit [km] for 4.3 bps SKR | 17 | 10.5 | 17 | | | 10.5 | | 10 |
| Distance limit [km] for 0.83 bps SKR | 17 | 10.5 | 17 | | | 10.5 | | |

**Tabela 4.1:** *Desempenho do DV-QKD BB84 em configurações de fibra escura/compartilhada P2P/P2MP. A tabela indica as limitações de distância para taxas de chave segura (Secure Key Rate - SKR) e os rigorosos requisitos de atraso em redes fronthaul 5G (distâncias de até 17 km). Fonte: Quantum Cryptography in 5G Network [Mehic* et al. *2024].*

Além disso, os autores investigaram topologias híbridas P2MP/*Fiber-Wi-Fi* (Fi-Wi), combinando uma rede P2MP em fibra compartilhada com enlaces sem fio em malha (*mesh*) por ondas milimétricas. Nesse caso, cada nó final da topologia P2MP se conecta a até quatro nós finais adicionais via enlaces sem fio com feixes ultrafinos. Essa configuração Fi-Wi permitiu aumentar a distância máxima de transmissão viável em aproximadamente 5 a 6 km em relação à topologia somente em fibra compartilhada P2MP.

### 4.1.4 Estudo de caso 2

Em [Milovančev 2021], os autores demonstraram o desempenho de um sistema *CV-QKD* (*Continuous-Variable - QKD*) aplicado a uma rede *fronthaul* 5G. Diferente do *DV-QKD*, que depende de detectores de fóton único , lentos e de custo elevado, o *CV-QKD* utiliza a natureza ondulatória da luz e pode ser implementado com detectores homódinos balanceados comerciais, alcançando altas taxas de geração de chaves secretas.

Nas redes *fronthaul* móveis 5G, a técnica de Multiplexação por Divisão de Comprimento de Onda (*Wavelength Division Multiplexing* - WDM) é amplamente usada para atender a maiores demandas de largura de banda. Os autores mostraram que uma rede óptica passiva (PON) baseada em WDM pode ser reutilizada para integrar *CV-QKD* em paralelo aos canais clássicos existentes. Conforme a arquitetura proposta (Fig. 4.4), um único transmissor quântico (estação Alice), localizado na unidade centralizada dentro do CO, é compartilhado no tempo entre vários receptores quânticos (estações Bob) localizados em diferentes locais de antena. Essa integração ocorre por meio de comutação espacial no CO e multiplexação espectral.

A Figura 4.4 ilustra a integração de um sistema *CV-QKD* em uma rede fronthaul mó-

vel 5G baseada em PON e WDM. Um único transmissor quântico (Alice), localizado na unidade centralizada do CO, distribui chaves secretas para múltiplos receptores (Bobs) situados em diferentes locais de antena. A multiplexação espectral permite que canais quânticos e clássicos coexistam na mesma fibra, enquanto a comutação espacial no CO garante que o transmissor possa atender a vários receptores em diferentes horários. Essa abordagem explora a natureza ondulatória da luz, usando detectores homódinos balanceados comerciais, aumentando a taxa de geração de chaves em comparação com detectores de fóton único, típicos de sistemas DV-QKD.

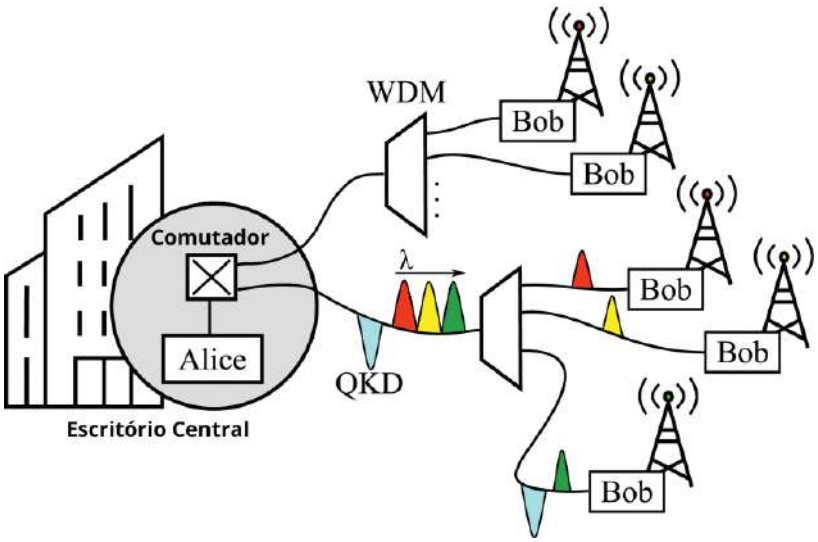



**Figura 4.4:** *Rede fronthaul móvel 5G protegida por QKD. Fonte: Adaptado de Quantum Cryptography in 5G Network [Mehic* et al. *2024].*

Os autores estimaram uma taxa de chave secreta necessária de aproximadamente 10 Mbps, considerando um tempo de sincronização de 5 segundos por par transmissor-receptor e os parâmetros de rede de acesso (cobertura de 4.000 macrocélulas e 48.000 pequenas células dentro do CO) listados na Tabela 4.2. Cada par também necessitou armazenar cerca de 200 Mb de material de chave quântica para lidar com períodos de inatividade devido à sincronização.

| Network resource | Scenario / Characteristic | Macro-cell | Small cell |
|---|---|---|---|
| Remote Radio Head | Data rate per beam | 20 Gbps | 100 Gbps |
| | Number of beams | 5 | 1 |
| Antenna site | Number of sectors | 3 | 1 |
| | Inter-site distance | 200 m | - |
| | Small cells per macro-cell sector | 4 | - |
| Mobile fronthaul | Range | 20 km | |
| | Data channel allocation | C-band | |
| QKD | AES lifetime | 64 Gbyte | |
| | Quantum channel allocation | C-band | |

**Tabela 4.2:** *Parâmetros da rede de acesso rádio utilizados no estudo de CV-QKD. Fonte: Quantum Criptography in 5G Networks: A comprehensive Overview [Mehic* et al. *2024]*

Os testes em um link fronthaul de 13,2 km mostraram que as taxas de chave secreta obtidas excederam 10 Mbps. Para um link escuro com modulação *Gaussiana* ou *Nyquist*, as taxas de chave secreta alcançaram 12 e 18,4 Mbps, respectivamente, mesmo assumindo um cenário adverso em que um espião controlasse o ruído do detector. Durante a transmissão conjunta na banda C, sinais quânticos e clássicos causaram uma leve redução nas taxas de chave secreta, resultando em 9,6 e 10,7 Mbps, ainda dentro das exigências da rede. Como os receptores quânticos estão geralmente em locais seguros e confiáveis, taxas ainda mais altas são possíveis, indicando grande potencial para suportar redes fronthaul 5G com integração *QKD* econômica.

| Quantum signal Characteristics | $R_q$=250 MHz Gauss-shaped | | $R_q$=500 MHz Nyquist-shaped | |
|---|---|---|---|---|
| Number of classic channels | 0 | 11 | 0 | 11 |
| Key rate $K_S$ [Mbps] | 12 | 9.59 | 18.4 | 10.7 |
| Key rate $K_T$ [Mbps] | 43.2 | 38.9 | 85.3 | 72 |

**Tabela 4.3:** *Desempenho do CV-QKD em um link de fronthaul com alcance de 13,2 km. Fonte: Quantum Cryptography in 5G Network [Mehic* et al. *2024].*

### 4.1.5 Estudos intimamente relacionados

Alguns estudos não tratam diretamente de redes *fronthaul* móveis 5G habilitadas para *QKD*, mas investigam redes de acesso habilitadas para *QKD* em geral. Apesar do foco distinto, há similaridades na tecnologia óptica utilizada para implantar essas redes, o que justifica apresentá-los aqui. A seguir, descrevem-se brevemente alguns desses trabalhos, com ênfase

nas abordagens adotadas para implementar redes de acesso quânticas e nas taxas de chave alcançáveis.

Em Fröhlich (2015, apud [Mehic *et al.* 2024]), foi demonstrada a integração de uma rede de acesso quântico *upstream* em uma *Gigabit* PON (GPON) com canais de dados em potência total. Um esquema de Multiplexação por Divisão de Tempo (*Time Division Multiplexing* - TDM foi usado para multiplexar sinais quânticos *upstream* de vários transmissores para um único receptor quântico. A alocação espectral utilizada foi: canal quântico em 1550 nm, sinal de *clock* em 1610 nm e sinais GPON em 1310 nm (*upstream*) e 1490 nm (*downstream*). Foram obtidas SKRs positivas em uma rede de acesso quântico suportando até 128 nós finais, limitada a 20 km de distância (equivalente à distância máxima de um link fronthaul 5G sem proteção). Para isso, utilizou-se uma configuração de fibra alimentadora dupla, em que o canal quântico é atribuído a um alimentador dedicado, reduzindo o ruído proveniente do espalhamento Raman. Em plena capacidade (transmissores operando a 1 GHz/128), o SKR por usuário foi inferior a 0,01 kbps; já com 16 nós finais, atingiu aproximadamente 10 kbps.

Os princípios teóricos da integração de *QKD* em Fibra *Multicore* (MCF) para redes de acesso de rádio seguras foram apresentados em Llorente et al. (2018, apud [Mehic *et al.* 2024]). Posteriormente, uma rede de acesso quântico baseada em MCF foi demonstrada em Cai (2019, apud [Mehic *et al.* 2024]), onde a MCF foi empregada como fibra alimentadora. Para viabilizar economicamente a integração, o canal quântico foi multiplexado com canais clássicos na mesma fibra. Para reduzir os efeitos do espalhamento Raman e da diafonia entre núcleos, os autores propuseram um esquema de atribuição de núcleo e comprimento de onda, dedicando um núcleo exclusivo ao canal quântico e alocando o espectro em comprimentos de onda inferiores a 1540 nm. Esse arranjo resultou em menor QBER. Os autores mostraram que o esquema TDM não era ideal, pois a velocidade do transmissor diminuía com o aumento do número de nós finais e divisores adicionais introduziam ruído. O uso isolado de WDM resultaria em desperdício de espectro, portanto propuseram um esquema combinado de WDM e TDM para sinais quânticos. Nessa integração, SKRs de até 1,64 kbps foram alcançadas a 20 km, podendo ser ampliadas com a adição de mais receptores quânticos.

Em Wang (2021, apud [Mehic *et al.* 2024]), foi apresentada uma rede de acesso quântico *downstream* em uma Rede Óptica Passiva *Ethernet* de 10 Gbps (10G-EPON). Comparada à configuração *upstream*, a configuração *downstream* apresentou menor ruído no canal quântico, possibilitando SKRs maiores. Usando uma estrutura de fibra alimentadora única, obteve-se um SKR de 1,5 kbps por usuário a 21 km em uma rede com 16 nós finais, porém os sinais 10G-EPON foram atenuados em 9 dB para alcançar essa distância. Já com uma fibra alimentadora dupla, a rede suportou 64 nós finais com sinais 10G-EPON em potência total em uma distância de 11 km. Os autores também propuseram um esquema de divisor de potência dupla para permitir SKRs configuráveis.

# Capítulo 5

# Resultados e Conclusão

Este Trabalho analisou o artigo *Quantum Cryptography in 5G Networks: A Comprehensive Overview* [Mehic *et al.* 2024], destacando as aplicações da *QKD* como alternativa de segurança para redes 5G. O artigo explora como a crescente densificação, as exigências de baixa latência e o alto volume de tráfego das redes 5G impõem novos desafios de segurança que os métodos tradicionais como IPsec e MACsec não conseguem atender integralmente. Além disso, enfatiza que o uso de mecanismos criptográficos pode impactar o desempenho da rede, principalmente nos segmentos mais críticos, como o *fronthaul* óptico.

A *QKD* é apontada como uma solução promissora para prover segurança resistente a ataques futuros, já que suas garantias são baseadas em princípios da física quântica, e não em premissas computacionais. No entanto, a aplicação da *QKD* se mostra mais adequada a trechos fixos da rede, como enlaces ópticos *fronthaul*, onde o canal quântico pode ser implementado por meio de fibra escura ou infraestrutura compartilhada. Ainda assim, há limitações físicas de distância e interferência que impactam o desempenho do canal quântico.

O artigo também apresenta implementações práticas e propõe o uso de criptografadores dedicados, como os baseados em FPGA, para atender aos requisitos de baixa latência e recodificação frequente de chaves. Observou-se que os atrasos introduzidos por IPsec (56 bytes) e MACsec (32 bytes), mesmo com *hardware* otimizado, ainda podem comprometer a performance de enlaces sensíveis. Por isso, há ênfase na necessidade de desenvolver criptografadores com capacidade de suportar recodificação rápida e baixa variação de atraso para viabilizar a aplicação da *QKD* no contexto 5G.

Em suma, o artigo base conclui que, embora a *QKD* ainda enfrente desafios técnicos e de integração, ela representa uma solução viável e segura para proteger segmentos críticos de redes 5G. A expectativa é que, com o avanço das pesquisas e a popularização de equipamentos quânticos, a produção em escala de sistemas *QKD* torne-se possível, possibilitando sua adoção em redes de telecomunicações com requisitos de segurança cada vez mais rigorosos.

Embora o artigo base também discuta abordagens de Criptografia Pós-Quântica (PQC), este Trabalho não realizou uma análise detalhada dessas técnicas, uma vez que o escopo definido concentrou-se exclusivamente na aplicação da *QKD* em redes 5G. A ausência de

comparações diretas com a PQC decorre, portanto, da delimitação temática adotada. Ainda assim, reconhece-se que um confronto sistemático entre as limitações da *QKD* (como alcance restrito, dependência de canal quântico e desafios de integração) e as características da PQC (baseada em algoritmos clássicos e viável em canais convencionais) pode oferecer uma visão mais abrangente do panorama de segurança quântica. Tal comparação é recomendada como continuidade para trabalhos futuros, de modo a avaliar como essas tecnologias podem se complementar na proteção de redes de telecomunicações.

A Figura 5.1 sintetiza a aplicação prática da *QKD* em redes 5G, ilustrando a integração de criptografadores e sistemas de gerenciamento de chaves ao longo das diferentes camadas da rede. Nota-se que a maior aplicabilidade ocorre no *fronthaul*, devido à baixa latência e enlaces ópticos de curta distância, mas também há cenários possíveis no *midhaul* e *backhaul*, desde que respeitadas as limitações físicas da transmissão quântica.

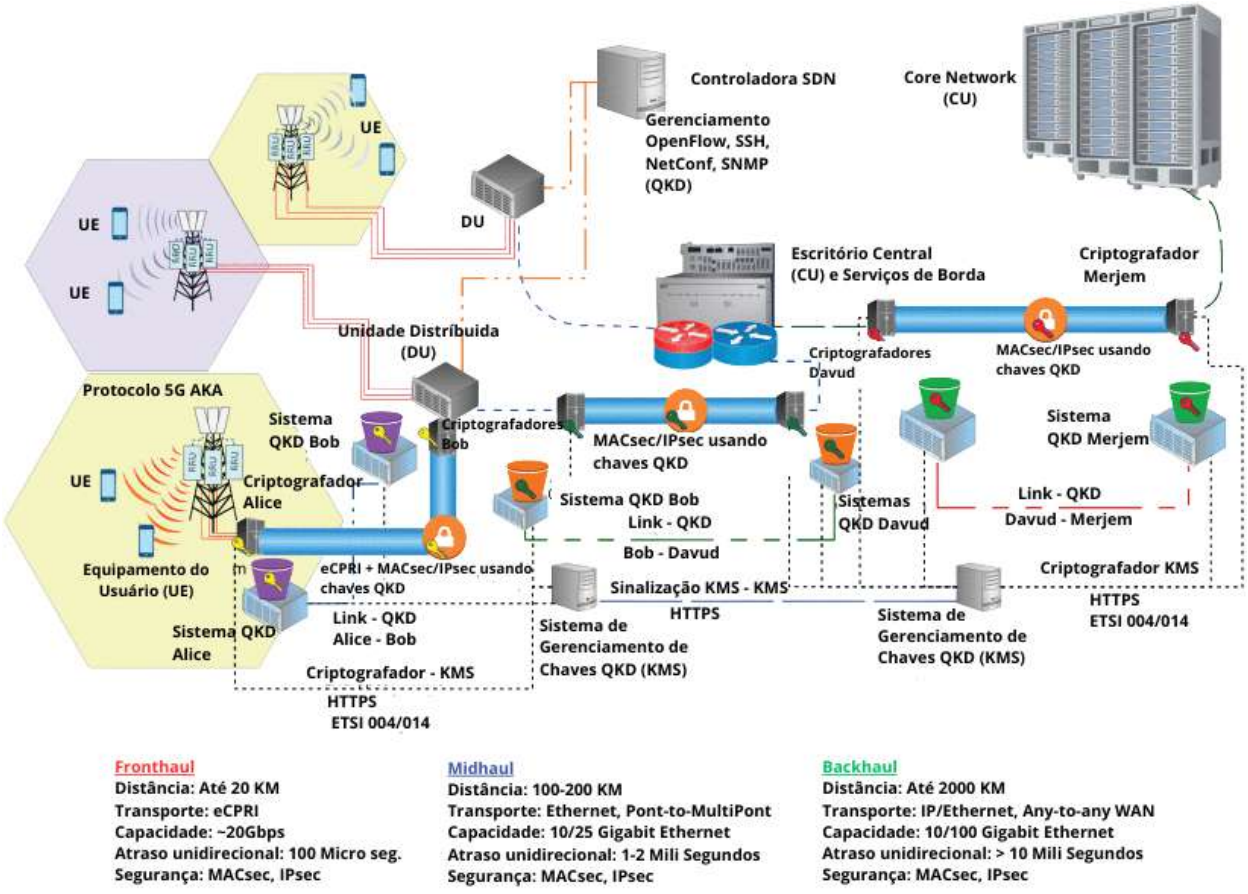



**Figura 5.1:** *Aplicação da QKD em uma rede 5G, destacando os segmentos de fronthaul, midhaul e backhaul. Fonte: Adaptado de Quantum Cryptography in 5G Networks [Mehic* et al. *2024].*

## 5.1 Sugestões para Trabalhos Futuros

Como este Trabalho teve como objetivo analisar o artigo [Mehic *et al.* 2024] e compreender as aplicações da *QKD* no contexto das redes 5G, entende-se que ainda há diversas possibilidades de aprofundamento.

Um caminho natural para trabalhos futuros é ampliar o estudo detalhado sobre a própria tecnologia *QKD*, principalmente nos aspectos técnicos que ainda apresentam desafios, como a limitação de distância dos enlaces quânticos, o impacto do espalhamento Raman em fibras compartilhadas e o desenvolvimento de criptografadores especializados que atendam às exigências de baixa latência e alta taxa de recodificação de chaves. Explorar novas propostas de *QKD*, como os esquemas de campo duplo e soluções baseadas em chip, também se mostra relevante, dado o potencial de compactação e eficiência energética que essas arquiteturas oferecem.

Outro ponto importante consiste em investigar abordagens híbridas que combinem *QKD* e PQC, avaliando como essas técnicas podem se complementar para oferecer maior resiliência em cenários de redes heterogêneas. Além disso, recomenda-se aprofundar a análise da padronização e da interoperabilidade de sistemas *QKD*, considerando os esforços atuais de organismos internacionais como o ETSI e o ITU-T.

Também se sugere a realização de simulações de cenários práticos de aplicação da *QKD* em redes 5G, de modo a avaliar o impacto da tecnologia em diferentes topologias e requisitos de desempenho, sem limitar-se a uma ferramenta específica, mas buscando compreender sua aplicabilidade em ambientes reais de telecomunicações.

Portanto, como continuidade deste trabalho, o objetivo será investigar com maior profundidade a evolução da *QKD*, com foco em sua integração prática, na complementaridade com outras tecnologias de segurança e na análise de cenários simulados, de modo a garantir proteção avançada e desempenho adequado às exigências não apenas das redes 5G, mas também das futuras redes rumo ao 6G.

# Referências Bibliográficas


[3GPP 2020] 3GPP, D. System architecture for the 5g system (5gs). *3rd Generation Partnership Project (3GPP), Technical Specification (TS)*, v. 23, n. 501, 2020. 6

[Ahmad *et al.* 2018] AHMAD, I. *et al.* Overview of 5g security challenges and solutions. *IEEE Communications Standards Magazine*, v. 2, n. 1, p. 36–43, MARCH 2018. ISSN 2471-2833. 8, 9

[Al-obaidi *et al.* 2015] AL-OBAIDI, R. *et al.* Optimizing cloud-ran deployments in real-life scenarios using microwave radio. In: IEEE. *2015 European Conference on Networks and Communications (EuCNC)*. [S.l.], 2015. p. 159–163. 6

[Alleaume 2014] ALLEAUME, R. Using quantum key distribution for cryptographic purposes: A survey. *Theoretical Computer Science*, v. 560, n. Part 1, p. 62–81, dez. 2014. 17

[Arfaoui *et al.* 2018] ARFAOUI, G. *et al.* A security architecture for 5g networks. *IEEE Access*, v. 6, p. 22466–22479, 2018. ISSN 2169-3536. 9

[Bennett e Brassard 1984] BENNETT, C. H.; BRASSARD, G. Quantum cryptography: Public key distribution and coin tossing. In: *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*. Bangalore, India: [s.n.], 1984. v. 175, p. 175–179. 10, 11

[Bennett e Brassard 1984] BENNETT, C. H.; BRASSARD, G. An update on quantum cryptography. In: *Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques*. [S.l.: s.n.], 1984. p. 475–480. 10

[Bethune e Risk 2000] BETHUNE, D. S.; RISK, W. P. An autocompensating fiber-optic quantum cryptography system based on polarization splitting of light. *IEEE Journal of Quantum Electronics*, v. 36, n. 3, p. 340–347, Mar 2000. 14

[Bjømstad, Chen e Veisllari 2018] BJØMSTAD, S.; CHEN, D.; VEISLLARI, R. Handling delay in 5g ethernet mobile fronthaul networks. In: *2018 European Conference on Networks and Communications (EuCNC)*. [S.l.: s.n.], 2018. p. 1–9. 42

[Cho, Sergeev e Zou 2019] CHO, J. Y.; SERGEEV, A.; ZOU, J. Securing ethernet-based optical fronthaul for 5g network. In: *Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES)*. [S.l.: s.n.], 2019. p. 1–6. 27

[Chowdhury 2020] CHOWDHURY, A. *The Impact Of 5G Network On Industry 4.0*. 2020. xvi, 4, 5

[Constantin *et al.* 2017] CONSTANTIN, J. *et al.* An fpga-based 4mbps secret key distillation engine for quantum key distribution systems. *Journal of Signal Processing Systems*, v. 86, p. 1–15, jan. 2017. 16

[Dianati e Alléaume 2007] DIANATI, M.; ALLéAUME, R. Architecture of the secoqc quantum key distribution network. In: *Proceedings of the 1st International Conference on Quantum, Nano and Micro Technologies (ICQNM)*. [S.l.: s.n.], 2007. p. 13. 18

[Gil 2008] GIL, A. C. *Métodos e técnicas de pesquisa social*. 6. ed. [S.l.]: Atlas, 2008. 35

[Gisin *et al.* 2002] GISIN, N. *et al.* Quantum cryptography. *Reviews of Modern Physics*, v. 74, n. 1, p. 145–195, mar. 2002. 14

[Huttner *et al.* 1995] HUTTNER, B. *et al.* Quantum cryptography with coherent states. *Physical Review A*, v. 51, n. 3, p. 1863–1869, 1995. 14

[International Telecommunication Union 2020] International Telecommunication Union. *IMT Vision - Framework and overall objectives of the future development of IMT for 2020 and beyond*. [S.l.], 2020. Disponível em: <https://www.itu.int/rec/R-REC-M.2083/en>. 4

[Khan *et al.* 2020] KHAN, R. *et al.* A survey on security and privacy of 5g technologies: Potential solutions, recent advancements, and future directions. *IEEE Communications Surveys Tutorials*, v. 22, n. 1, p. 196–248, Firstquarter 2020. ISSN 1553-877X. 9

[Larsen, Checko e Christiansen 2018] LARSEN, L. M.; CHECKO, A.; CHRISTIANSEN, H. L. A survey of the functional splits proposed for 5g mobile crosshaul networks. *IEEE Communications Surveys & Tutorials*, IEEE, v. 21, n. 1, p. 146–172, 2018. 6

[Makarov e Hjelme 2005] MAKAROV, V.; HJELME, D. R. Faked states attack on quantum cryptosystems. *Journal of Modern Optics*, v. 52, n. 5, p. 691–705, 2005. 14

[Mehic *et al.* 2024] MEHIC, M. *et al.* Quantum cryptography in 5g networks: A comprehensive overview. *IEEE Communications Surveys  Tutorials*, v. 26, p. 302–346, 12 2024. ISSN 1553-877X. xvi, xvii, xviii, 1, 5, 6, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 36, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49

[Mehic *et al.* 2017] MEHIC, M. *et al.* Analysis of the public channel of quantum key distribution link. *IEEE Journal of Quantum Electronics*, v. 53, n. 5, p. 99–106, 2017. 16

[Milovančev 2021] MILOVANčEV, D. High rate cv-qkd secured mobile wdm fronthaul for dense 5g radio networks. *Journal of Lightwave Technology*, v. 39, n. 11, p. 3445–3457, jun. 2021. 44

[Minayo 2012] MINAYO, M. C. d. S. Análise qualitativa: teoria, passos e fidedignidade. *Ciência & Saúde Coletiva*, v. 17, n. 3, p. 621–626, 2012. 35

[Mink 2007] MINK, A. Custom hardware to eliminate bottlenecks in qkd throughput performance. In: *Proceedings of SPIE — Quantum Communications Realized*. Boston, MA: [s.n.], 2007. v. 6780, p. 191–196. 16

[Salvail 2010] SALVAIL, L. Security of trusted repeater quantum key distribution networks. *Journal of Computer Security*, v. 18, n. 1, p. 61–87, 2010. 17

[Wu *et al.* 2018] WU, Y. *et al.* A survey of physical layer security techniques for 5g wireless networks and challenges ahead. *IEEE Journal on selected areas in communications*, IEEE, v. 36, n. 4, p. 679–695, 2018. 8

[Yang *et al.* 2015] YANG, N. *et al.* Safeguarding 5g wireless communication networks using physical layer security. *IEEE Communications Magazine*, v. 53, n. 4, p. 20–27, April 2015. ISSN 1558-1896. 8

[Zavitsanos *et al.* 2020] ZAVITSANOS, D. *et al.* On the qkd integration in converged fiber/wireless topologies for secured, low-latency 5g/b5g fronthaul. *Applied Sciences*, v. 10, n. 15, p. 5193, 2020. 43

**INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DA PARAÍBA**
Campus Campina Grande - Código INEP: 25137409
R. Tranqüilino Coelho Lemos, 671, Dinamérica, CEP 58432-300, Campina Grande (PB)
CNPJ: 10.783.898/0003-37 - Telefone: (83) 2102.6200

# Documento Digitalizado Restrito

## Trabalho de Conclusão de Curso

| | |
|---|---|
| **Assunto:** | Trabalho de Conclusão de Curso |
| **Assinado por:** | Mikael Marinho |
| **Tipo do Documento:** | Projeto |
| **Situação:** | Finalizado |
| **Nível de Acesso:** | Restrito |
| **Hipótese Legal:** | Informação Pessoal (Art. 31 da Lei no 12.527/2011) |
| **Tipo do Conferência:** | Cópia Simples |

Documento assinado eletronicamente por:

- **Mikael Marinho Oliveira**, **DISCENTE (202211210036) DE TECNOLOGIA EM TELEMÁTICA - CAMPINA GRANDE**, em 18/08/2025 10:44:23.

Este documento foi armazenado no SUAP em 18/08/2025. Para comprovar sua integridade, faça a leitura do QRCode ao lado ou acesse https://suap.ifpb.edu.br/verificar-documento-externo/ e forneça os dados abaixo:

Código Verificador: 1577122
Código de Autenticação: 7f20a03acc