

Integração Prática de Distribuição Quântica de Chaves com IPsec: Prova de Conceito em Aplicação de Interesse Militar

Denys Derlian Carvalho Brito¹, Igor José Sleutjes², Caio Augusto de Melo Arruda Silvestre²,
Romildo Henrique de Souza¹, Felipe Streintberger Ivo¹, Rui Andrade Carvalho Nunes¹,
Bruno Simões Nagem¹, Leonardo Xavier Dantas¹, Renato Machado¹, Felix Dieter Antreich¹,
Lucio Pinheiro Amaro¹, Edison Puig Maldonado¹.

¹Instituto Tecnológico de Aeronáutica (ITA), São José dos Campos/SP – Brasil,

²Instituto de Aplicações Operacionais (IAOp), São José dos Campos/SP – Brasil.

Resumo – A segurança de comunicações sensíveis depende da robustez dos algoritmos e da gestão do ciclo de vida das chaves. Este artigo apresenta a integração entre Distribuição Quântica de Chaves (QKD) e IPsec na demonstração Link Quântico Operacional, conduzida pelo CCGE/ITA em cooperação com o IAOp. O enlace utilizou 4276(2) m de fibra óptica, com separação dos planos quântico, de serviço, de gerenciamento de chaves e de dados, integrando nós QKD comerciais e gateways próprios. A implementação combina uma PSK fixa para autenticação dos pares com chaves QKD sincronizadas por identificadores públicos e incorporadas ao IKEv2 como PPKs (*Post-Quantum Preshared Keys*, conforme a RFC 8784), renovadas a 1 Hz. Assim, o material QKD participa da derivação das chaves de tráfego IPsec. A demonstração evidencia competências de integração de sistemas do Laboratório de Fotônica para Tecnologias Quânticas do ITA e estabelece uma plataforma experimental replicável para pesquisa e formação de recursos humanos.

Palavras-Chave – Criptografia, QKD, IPsec, ETSI 014

I. INTRODUÇÃO

Em comunicações sensíveis, a escolha de algoritmos para máxima robustez na cifragem de dados, assim como de *hardware* e sistema, não resolve de forma definitiva o problema de segurança. A efetividade operacional depende do ciclo de vida completo das chaves criptográficas, o que inclui sua geração, distribuição, armazenamento, período autorizado de uso, auditoria, substituição e destruição. Esse intervalo autorizado normalmente é chamado *cryptoperiod*, sendo definido conforme o algoritmo, a aplicação, o volume de tráfego, a sensibilidade da informação e a ameaça considerada [1]. Embora surjam novas ameaças à segurança da comunicação criptografada, considera-se que esquemas simétricos e autenticados de criptografia, tais como o AES-GCM, continuam adequados para proteção eficiente de dados, desde que acoplados a políticas rigorosas de autenticação, integridade e renovação de chaves [2].

O avanço da computação quântica representa ameaça severa à criptografia assimétrica convencional, em especial diante da possibilidade futura de computadores quânticos criptograficamente relevantes. Algoritmos como RSA e criptografia de curvas elípticas (ECC), que sustentam grande parte das comunicações seguras modernas, são vulneráveis a algoritmos quânticos de tempo polinomial para fatoração e logaritmos discretos [3]. Nesse contexto, a Distribuição Quântica de Chaves (QKD, *Quantum Key Distribution*) surge

como abordagem baseada em *hardware* para estabelecer chaves criptográficas à distância. Sob hipóteses explícitas de modelagem e implementação, protocolos QKD podem oferecer, para o estabelecimento de chaves, segurança informacional fundamentada em leis físicas e não em dificuldade computacional. Essa propriedade refere-se ao modelo do protocolo QKD e não à segurança dos componentes clássicos do sistema. Protocolos QKD também permitem detectar estatisticamente perturbações compatíveis com tentativa de interceptação, acompanhando eventual aumento de erros no canal quântico.

A relevância prática da QKD não está em substituir algoritmos e protocolos criptográficos clássicos, como AES, TLS, MACsec ou IPsec [4], mas em fornecer uma fonte física adicional de geração e renovação de chaves simétricas, com segurança condicionada ao modelo de segurança, à implementação e ao monitoramento operacional, para enlaces fixos de alto valor estratégico. Em infraestruturas críticas, órgãos de governo, data centers, centros de comando, bases militares e enlaces entre organizações operacionais, essa camada adicional contribui para defesa em profundidade, diversificação tecnológica e redução da exposição a ataques do tipo “*store now, decrypt later*” [1]. Diversos protocolos QKD foram propostos [5], demonstrados seguros sob hipóteses explícitas de modelagem e experimentalmente validados [6], [7]. O protocolo BB84, baseado em esquema de preparação e medição, é considerado canônico [8]. Frequentemente, é implementado como BB84 com estados isca (*decoy-state BB84*) [9]. Destacamos também a relevância atual (em pesquisa, projetos e implementações) dos protocolos QKD de variáveis contínuas (CV-QKD) [10], QKD independente de dispositivos de medição (MDI-QKD) [11] e QKD do tipo *coherent one-way* (COW), este último oferecendo importante equilíbrio entre segurança e simplicidade de implementação [12]. COW foi adotado pela empresa suíça *ID Quantique* na plataforma *Cerberis* [13], uma das soluções comerciais disponíveis para geração e gerenciamento de chaves QKD.

Apesar da maturidade teórica e da disponibilidade comercial de sistemas QKD, persiste uma lacuna entre compreensão teórica e integração em infraestruturas de rede existentes. Muitos estudos enfatizam o comportamento da camada física e os modelos de segurança dos protocolos de estabelecimento/distribuição de chaves, enquanto a questão operacional de integrar material de chave produzido por QKD a pilhas padronizadas de segurança de rede permanece menos transparente para profissionais [6]. Essa lacuna é particularmente visível na camada de gerenciamento de chaves, que envolve armazenamento, retransmissão de chaves em cenários com nós de rede confiáveis e interfaces para aplicações [14], [15].

Este artigo aborda orquestração de *software*, extração de material de chave por interfaces padronizadas e configuração dinâmica de políticas de tunelamento IPsec, com interações de entrega de chaves no perfil REST da ETSI GS QKD 014, abstraindo a camada física quântica [16].

Reportamos aqui uma implementação experimental de enlace IPsec com geração e renovação de chaves apoiadas por QKD, concebida como prova de conceito acadêmica em aplicação de interesse militar. O experimento, denominado Link Quântico Operacional (LQO), foi realizado em 3 de junho de 2026 pelo Centro de Competência em Guerra Eletrônica (CCGE) do Instituto Tecnológico de Aeronáutica (ITA), em cooperação com o Instituto de Aplicações Operacionais (IAOp). Chaves obtidas do sistema QKD e aplicadas como PPKs, renovadas à taxa de 1 Hz, foram utilizadas para avaliar a integração entre QKD, KMS e IPsec em cenário de tráfego associado a sinais de radar. O objetivo principal foi apoiar a implantação e validação didática do Laboratório de Fotônica para Tecnologias Quânticas (LTQ) do CCGE/ITA, no escopo do projeto INFREQUANT [17], com ênfase em simplicidade, replicabilidade, apoio à formação de recursos humanos e não no endurecimento para produção ou operação continuada.

II. TOPOLOGIA DE REDE E ARQUITETURA

O ambiente experimental compreendeu uma arquitetura lógica de três nós gerenciais, com uma estação de orquestração e nós QKD *Alice* e *Bob*, isolada dos canais ativos de comunicação, que estão em rede própria com os nós *Gateway Alice* e *Gateway Bob* (ambos com sistemas Debian), que por sua vez estão também conectados às redes A e B. O *hardware* responsável pela geração de chaves é o sistema *Cerberis*, da *ID Quantique*, integrado ao sistema de gerenciamento de chaves (KMS) *Clarion*. O *Cerberis* estabelece o canal quântico óptico unidirecional de *Alice* para *Bob* e executa pós-processamento clássico, incluindo *sifting*, correção de erros e amplificação de privacidade. As conexões ópticas principais da atividade foram implementadas com comprimento de fibra de 4276(2) m. A Figura 1 apresenta um diagrama de alto nível dessas conexões.

Visando clareza e didatismo, a arquitetura de *software* utiliza uma abordagem com duas aplicações *desktop*, desenvolvidas com PyQt6. Essas interfaces interagem diretamente com as *Key Management Entities* (KMEs) definidas por perfis de aplicação QKD e APIs de entrega de chaves do ETSI em *endpoints* REST específicos [16], [18]. Os *endpoints* IPsec atuam como *Security Application Entities* (SAEs), que solicitam material de chave às KMEs locais por interfaces padronizadas [16], [18].

De forma mais ampla, a ITU-T caracteriza essa interação como uma rede QKD que fornece chaves a aplicações criptográficas por meio de uma fronteira de demarcação de segurança, cabendo ao gerenciamento de chaves o armazenamento seguro, a retransmissão opcional e o controle de ciclo de vida [15]. A orquestração proposta preserva essa separação: o PC de gerenciamento coordena temporização e visualização de estado, mas o material secreto de chave é buscado apenas localmente em cada *endpoint* [14].

No cenário experimental de interesse militar considerado, a atividade LQO deve ser interpretada como uma integração de sistemas. A arquitetura organizada pelo CCGE-ITA contemplou a separação entre canal quântico, canal de serviço, canal KMS, canal de gerenciamento, canal de informação cifrada e canal destinado a sinais de radar, com o IAOp fornecendo o contexto de aplicação para avaliação acadêmica da aplicabilidade [19]. A prova de conceito organiza uma arquitetura completa, com planos quântico, KMS, gerenciamento e dados separados.

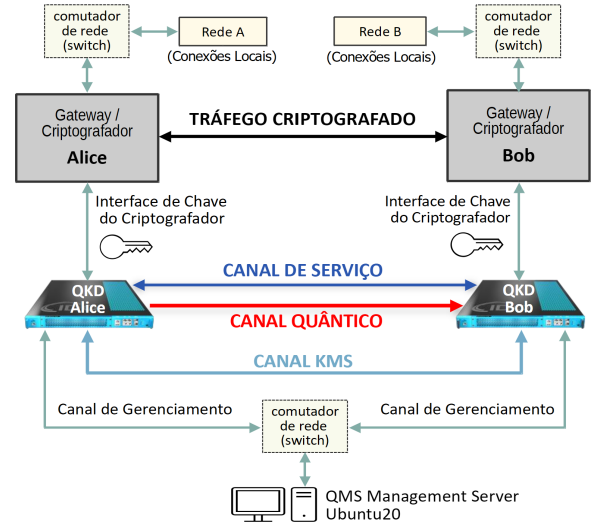


Figura 1. Diagrama de rede de alto nível representando as conexões entre o PC de gerenciamento, Alice e Bob, incluindo o fluxo de chaves e dados.

III. METODOLOGIA DE IMPLEMENTAÇÃO

A cadeia de *software* que conecta a KME QKD a um túnel IPsec foi implementada enfatizando reprodutibilidade e separação entre identificadores públicos para sincronização e o material simétrico de chave usado pelos cifradores.

A. Entrega de chaves via ETSI GS QKD 014

A aquisição de chaves é realizada pela API REST de entrega de chaves da ETSI GS QKD 014 [16]. Em Alice, o controlador envia uma requisição HTTPS POST ao *endpoint* da KME solicitando uma chave simétrica de 256 bits e recebe uma resposta JSON contendo o valor da chave codificado em Base64 e um *key_ID* associado. Em Bob, o controlador utiliza o *key_ID* recebido para consultar a KME local e recuperar, localmente, o material de chave correspondente.

O uso do *key_ID* como identificador público é central para evitar exposição acidental de chaves: o identificador permite que os pares referenciem o mesmo material de chave sem transportá-lo entre *endpoints* e oferece suporte a auditoria e operações de ciclo de vida, como alocação, consumo e expiração [14], [15].

Esse modelo de entrega por API desacopla a geração do consumo de chaves e se alinha a propostas recentes que expõem serviços quânticos por interfaces REST padronizadas, incluindo cenários orientados a nuvem baseados em ETSI GS QKD 004/014 [16], [18], [20].

Na implementação de referência, essas interações são encapsuladas em *scripts* de *shell* executados por *threads* de trabalho da interface gráfica. Os *scripts* são parametrizados exclusivamente por variáveis de ambiente, incluindo *host* e porta da KME, identificador SAE e caminhos de certificados, permitindo a redistribuição com mínima alteração específica de topologia. O acesso às KMEs utiliza certificados X.509 de cliente, mas a validação do certificado do servidor foi desabilitada por conveniência laboratorial, limitando a autenticação mútua prevista [16], [18].

B. IPC fora de banda para sincronização do identificador

Após a obtenção de uma chave por Alice, apenas o *key_ID* é transmitido a Bob por um canal TCP/IP de comunicação entre processos (IPC) fora de banda, operando na porta 65432/TCP. Esse canal não transporta o material secreto da chave; ele apenas permite que Bob solicite à sua KME local a chave correspondente. Para fins didáticos, o canal IPC também transporta metadados mínimos de validação, como *hashes* truncados, para facilitar a visualização de concordância entre os *endpoints*.

Esse desenho separa a sincronização do plano de controle, baseada em identificador e metadados de validação, dos segredos do plano de dados. A separação corresponde à visão de gerenciamento de chaves na qual as aplicações trocam apenas os metadados mínimos necessários para solicitar e consumir chaves, enquanto o material de chave permanece confinado ao repositório confiável e ao *endpoint* [14], [15]. O mecanismo IPC fornece sincronização sem revelar o segredo.

C. Troca de chaves IPsec com StrongSwan

A Figura 2 mostra o esquema da arquitetura de *software*, com os nós e canais de comunicação. Nos dois nós, uma PSK fixa é mantida para autenticação dos pares. Chaves fornecidas pelo sistema QKD são instaladas como *Post-Quantum Preshared Keys* (PPKs) no StrongSwan por escrita no arquivo de configuração e recarregamento das credenciais no *daemon* Charon. Alice encerra a *IKE Security Association* (IKE SA) ativa e reinicia a conexão configurada, provocando nova negociação IKEv2 com a PPK atualizada. Conforme a RFC 8784 [21], a PPK, renovada a cada ciclo, é incorporada ao cálculo de SK_d , chave interna do IKEv2 utilizada para derivar o material criptográfico que protege o tráfego das *Child SAs*.

Independentemente de onde sejam injetadas no protocolo, o ciclo de vida operacional das chaves QKD é relevante: o plano de gerenciamento deve evitar reuso inadvertido, manter rastreabilidade e reconciliar disponibilidade de chaves com o cronograma de *rekey* [14], [15]. Sob essa perspectiva, a integração QKD-IPsec deve ser tratada como problema de gerenciamento de chaves, as quais podem ser derivadas dinamicamente, distribuídas por uma autoridade confiável ou pré-posicionadas antes da missão; cada alternativa envolve riscos distintos, como falha de autenticação, comprometimento da infraestrutura central, reuso, exaustão de reservas ou dificuldade logística de substituição [1]. A arquitetura IPsec, por sua vez, fornece associações de segurança e serviços de confidencialidade, integridade e autenticação no nível IP, enquanto o IKEv2 estabelece e

mantém essas associações [4], [22].

Como o estado IPsec é implementado no kernel Linux por meio do arcabouço XFRM, uma rotina de inicialização única é executada para interromper o StrongSwan, limpar tabelas de estado e de políticas XFRM, reiniciar o *daemon* e carregar perfis estáticos de conexão. Essa etapa reduz ambiguidades em experimentos, assegurando que o estado inicial do túnel seja de configuração corrente, e não de resíduos no kernel.

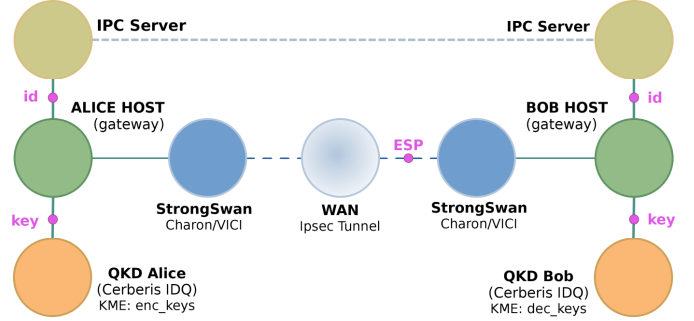


Figura 2. Esquema da arquitetura de *software*. Os gateways se conectam às KMEs por APIs REST e sincronizam identificadores de chave por IPC fora de banda. O túnel cifrado é estabelecido por StrongSwan.

IV. PROCEDIMENTO EXPERIMENTAL

O fluxo experimental é organizado em um laço periódico de *rekey* (neste artigo, entendido como o ciclo automatizado de encerramento e reestabelecimento da *IKE SA*) em Alice e de um laço orientado a eventos em Bob.

A. Ciclo de vida de uma rotação de chave

Primeiro, Alice solicita uma chave simétrica nova à KME local e extrai o *key_ID* e o valor da chave em Base64 retornados. Segundo, Alice envia o *key_ID* para Bob pelo canal TCP de IPC. Terceiro, ao receber o *key_ID*, Bob consulta sua KME local com um JSON que lista o identificador solicitado, obtendo localmente o material de chave correspondente [16]. Quarto, ambos os *endpoints* instalam a chave obtida como PPK no arquivo de configuração do StrongSwan e recarregam as credenciais, mantendo a PSK de autenticação fixa. Por fim, Alice encerra a *IKE SA* corrente e reinicia a conexão configurada, provocando nova negociação IKEv2 com a PPK atualizada, que participa da derivação das chaves de tráfego IPsec conforme a RFC 8784 [21].

B. Parâmetros de temporização e sincronização

Dois parâmetros de temporização são centrais para operação confiável no laboratório: o intervalo de *rekey* e o *timeout* de confirmação do IPC. Para testes, *rekey* foi ajustado para 20 s, valor suficientemente longo para concluir chamadas REST, troca IPC e operações de controle sem sobrepor ciclos sucessivos em *hardware* convencional. Também para testes, o *timeout* de IPC foi ajustado para 30 s, tolerando atrasos transitórios, como perda temporária de conexão IPC ou latência da KME, mas evitando bloqueio indefinido do laço de controle. Esses valores são conservadores por projeto e podem ser ajustados em função da carga do sistema e da postura de segurança desejada.

De forma mais geral, a temporização de *rekey* deve ser acoplada à taxa disponível de geração de chaves quânticas, ao consumo de chaves pela aplicação e às políticas de gerenciamento que governam alocação e expiração. A ITU-T trata o fornecimento de chaves como operação gerenciada através de uma fronteira de demarcação de segurança, e revisões recentes enfatizam que recursos de chave são limitados e precisam ser escalonados ao integrar serviços QKD a infraestruturas operacionais [14], [15]. Estratégias dinâmicas, como políticas de atualização por janela, foram propostas para acomodar variabilidade e escassez de chaves mantendo sincronização [24]. A Tabela I lista os parâmetros experimentais padrão usados pela pilha de orquestração.

No protótipo laboratorial descrito na Tabela I, o intervalo foi configurado em 20 s, mas na demonstração em enlace real do LQO, adotou-se renovação a 1 Hz, o que deve ser entendido como escolha de engenharia condicionada pela taxa de geração de chaves, latência das APIs, estabilidade do túnel e política de *cryptoperiod*. Rotações frequentes reduzem o volume de dados protegido por uma mesma chave e estreitam a janela de exposição em caso de comprometimento, mas exigem monitoramento da disponibilidade de entropia QKD e mecanismos de *fallback* para evitar indisponibilidade do serviço [1].

TABELA I. PARÂMETROS PADRÃO DE ORQUESTRAÇÃO (CONFIGURAÇÃO LABORATORIAL)

Parâmetro	Valor
Tamanho da chave (requisição KME)	256 bits
Intervalo de <i>rekey</i> (laço de Alice)	20 s
Porta IPC (Alice ↔ Bob)	65432/TCP
Timeout de confirmação IPC	30 s
Endpoints ETSI 014	enc_keys; dec_keys

V. RESULTADOS E DISCUSSÃO

Esta seção resume os resultados práticos da implementação e discute a caracterização experimental do canal quântico.

A. Artefatos de orquestração de *rekey* e observabilidade

A implementação fornece um plano de controle fim a fim que solicita chaves a uma KME pela interface ETSI GS QKD 014, sincroniza Alice e Bob por um canal IPC fora de banda que transmite o identificador de chave e metadados de validação, sem transmitir a própria chave, e instala o material obtido no StrongSwan como PPK a cada ciclo de renovação. Os registros do StrongSwan confirmaram a negociação com PPK nas conexões observadas.

O principal resultado didático é a observabilidade: cada evento de *rekey* é exposto por linhas de log estruturadas, transições de fase explícitas na interface gráfica e um mecanismo determinístico de verificação baseado em *hashes* truncados de chave. Na demonstração, o enlace permaneceu operacional por aproximadamente 180 min, abrangendo um número estimado da ordem de 10.000 ciclos de renovação. Seu funcionamento foi confirmado pela manutenção da funcionalidade da conexão protegida pelo túnel IPsec, utilizada para configuração e acionamento dos sinais de

radar, e pela recepção, no IAOp, do tráfego correspondente, sem interrupções perceptíveis na aplicação.

B. Caracterização de QBER em função da atenuação

Em implantações QKD, a *Quantum Bit Error Rate* (QBER) é comumente estudada como função da perda de canal. Sob perspectiva de sistemas, o aumento da atenuação reduz a relação sinal-ruído detectada, eleva o impacto relativo do ruído de detectores e aproxima a implementação dos limites básicos de taxa-perda de enlaces QKD [5], [7], [23].

Na prática, o crescimento da QBER afeta tanto a sobrecarga de correção de erros quanto a taxa de chave secreta alcançável, determinando frequentemente condições de aborto e margens de segurança quando estatísticas de tamanho finito e imperfeições de dispositivos são consideradas [6], [7]. Neste trabalho, o *software* de orquestração define procedimento repetível para adquirir chaves enquanto se varia a atenuação. Nos testes, foi medida a QBER em diferentes níveis de atenuação, com resultados apresentados na Figura 3. Cada ponto da curva foi obtido pela média de aproximadamente 1000 amostras consecutivas de QBER. A atenuação total do canal quântico, incluindo as perdas fixas e a atenuação introduzida por atenuadores ópticos, variou de 3 a 30 dB. Para cada medição, o sistema foi reinicializado para assegurar estado limpo.

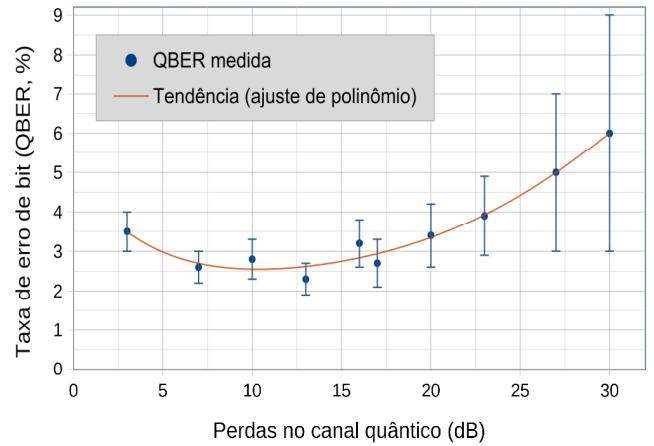


Figura 3. QBER medida em função da atenuação do canal, de aproximadamente 3 a 30 dB. Cada ponto da curva foi obtido pela média de aproximadamente 1000 amostras de QBER. As barras de erro representam o desvio padrão das medições; a atenuação corresponde à perda total do canal quântico; o ajuste polinomial serve apenas como guia visual.

Os resultados mostram o comportamento experimental esperado: à medida que a atenuação aumenta, a QBER cresce devido à redução da intensidade do sinal e ao aumento relativo do ruído. Uma pequena redução da QBER é visível aproximadamente entre 5 dB e 12 dB, possivelmente atribuível à otimização de condições de operação dos detectores, à supressão de efeitos de saturação, à melhoria de filtragem temporal ou a flutuações estatísticas. Em níveis de atenuação superiores a 20 dB, a QBER e a variância das medições aumentam, indicando maior incerteza estatística e redução das taxas de detecção de fóton.

A linha polinomial, apresentada apenas como guia visual, sugere uma região de menor QBER nas atenuações

intermediárias e crescimento do erro e da dispersão nas maiores perdas. A figura caracteriza o comportamento observado nas condições de teste, sem identificar isoladamente os mecanismos físicos responsáveis nem estabelecer, por si só, a segurança ou a taxa de chave secreta do enlace.

C. Restrições operacionais e compromissos de implementação

A abordagem priorizou facilidade de replicação e simplicidade em detrimento de endurecimento para produção. Primeiro, a aplicação de chaves ao StrongSwan depende de operações privilegiadas. Segundo, os *scripts* de obtenção de chaves desabilitam a validação do certificado TLS do servidor por conveniência laboratorial. Embora sejam utilizados certificados de cliente, essa configuração não assegura a autenticação mútua completa. Em ambientes operacionais, deve-se habilitar a validação do certificado do servidor com uma configuração de confiança adequada. Essas restrições indicam próximos passos claros rumo a um plano de controle apto ao emprego operacional, preservando as interações de API alinhadas ao ETSI [16], [18].

Em redes QKD, o gerenciamento de chaves também deve contemplar armazenamento seguro, fornecimento controlado e rastreabilidade do ciclo de vida do material gerado. Embora o protótipo use injeção da PPK em arquivo de configuração por transparência, implementações operacionais devem privilegiar interfaces seguras, alinhadas às orientações de gerenciamento de chaves de redes QKD [14], [15].

Do ponto de vista criptográfico, o protótipo deve ser interpretado, sobretudo, como artefato de orquestração e interoperabilidade: demonstra como chaves entregues por ETSI GS QKD 014 podem ser consumidas operacionalmente por uma pilha IPsec por eventos automatizados de *rekey*. Na configuração utilizada, as chaves QKD são incorporadas como PPKs conforme a RFC 8784, fazendo com que as chaves de tráfego IPsec dependam também desse material [21].

Arquiteturas como IPSeQ exploram acoplamento mais estreito entre disponibilidade de chaves quânticas, negociação e gerenciamento de associações de segurança [24]. A avaliação desse acoplamento constitui extensão futura da presente integração.

O resultado mais relevante foi comprovar a capacidade de proteger fluxo representativo de aplicação de interesse militar por uma infraestrutura que combina QKD, KMS, *gateways* e IPsec. O uso de *gateways* criptográficos próprios reforça o aspecto acadêmico do experimento, pois permite maior didatismo sobre a arquitetura, sobre a integração dos canais ópticos e sobre a política de consumo de chaves.

D. Posicionamento e limitações

A integração de QKD em pilhas operacionais de segurança é, essencialmente, um problema de engenharia de sistemas: equipamentos QKD geram material de chave sob restrições físicas de perda, taxa e estabilidade, enquanto protocolos como IPsec consomem chaves segundo regras próprias de negociação e renovação. Nesse contexto, interfaces padronizadas como ETSI GS QKD 014 e ETSI GS QKD 004, bem como modelos de gerenciamento de chaves QKDN,

são fundamentais para separar a geração quântica do consumo por aplicações clássicas [14]–[16], [18].

A prova de conceito apresentada diferencia-se de experimentos focados apenas em camada física por demonstrar o consumo de chaves QKD por uma pilha IPsec, com *gateways* próprios, sincronização por identificadores públicos e tráfego representativo de aplicação de interesse militar. Não se trata de sistema endurecido para produção: a implementação priorizou simplicidade, observabilidade, replicabilidade e valor didático, deixando como trabalhos futuros a validação estrita de certificados, o endurecimento do plano de controle, políticas formais de ciclo de vida de chaves e a avaliação de arquiteturas como IPSeQ [24].

Resultados recentes no Brasil e no hemisfério sul indicam diferentes graus de validação da tecnologia QKD. Demonstrações brasileiras divulgadas publicamente em fibra de longa distância, como o caso reportado do CPQD em Campinas [25], e estudos de longo prazo com equipamento comercial realizados pelo IME no Rio de Janeiro [26], enfatizam dimensões complementares de maturidade tecnológica. No cenário internacional próximo, destacam-se a demonstração australiana de CV-QKD em fibra AARNet/CSIRO [27] e a demonstração satelital entre China e África do Sul [28], [29]. O LQO contribui nesse panorama como referência acadêmica e replicável de integração QKD–KMS–IPsec em aplicação de possível interesse militar futuro.

VI. CONCLUSÃO

O LQO constituiu uma contribuição aplicada à integração de tecnologia QKD, e não um experimento de camada física ou sistema endurecido para produção, situando-se, até onde foi possível verificar, entre as primeiras provas de conceito regionais em aplicação de interesse militar. Empregando chaves distribuídas por canal quântico, a prova de conceito protegeu com sucesso o tráfego entre dois pontos do DCTA. Visou, em especial, consolidar procedimentos e funcionalidades de uso acadêmico no LTQ-CCGE/ITA, no escopo do projeto INFREQUANT [17]. A implementação demonstrou um fluxo de controle alinhado ao ETSI, que obtém chaves de uma KME por endpoints REST padronizados, sincroniza os endpoints por identificadores públicos e instala o material no StrongSwan como PPK, mantendo uma PSK fixa para autenticação dos pares. Conforme a RFC 8784 [21], o material QKD participa da derivação das chaves de tráfego IPsec. A renovação da PPK a 1 Hz acompanha o reestabelecimento periódico da *IKE SA*, combinando a contribuição do segredo QKD à derivação criptográfica com a redução do período de uso e do volume de dados protegido por cada chave.

A implementação oferece referência didática a profissionais interessados em integrar serviços QKD a pilhas de segurança de rede existentes. Demonstrou uma camada adicional de renovação e gestão de chaves para proteção de enlaces críticos em que a integração de QKD com IPsec pode apoiar cenários futuros de comando e controle, interligação segura entre organizações militares, redes de sensores e proteção de fluxos associados a sistemas operacionais sensíveis, desde

que acompanhada por políticas maduras de ciclo de vida, auditoria e contingência de chaves [1].

Assim, o valor comparativo desta prova de conceito não reside apenas na presença de QKD, já observada em outros testes experimentais no hemisfério sul, mas no acoplamento entre chaves quânticas, *gateways*, IPsec e tráfego associado a aplicação de interesse militar. Esse recorte posiciona o trabalho como referência de sistema didático de engenharia de integração no contexto de futuras redes com múltiplos enlaces, fornecedores e domínios de chaves. Embora os nós QKD sejam equipamentos comerciais de fornecedor estrangeiro, os *gateways*, o *software* de integração e a orquestração foram desenvolvidos ou integrados no âmbito do trabalho, ampliando o domínio da arquitetura e estabelecendo bases para maior autonomia tecnológica e futuro emprego operacional.

REFERÊNCIAS

- [1] NIST, “Recommendation for key management: Part 1 - General”, NIST Special Publication 800-57 Part 1 Revision 5, National Institute of Standards and Technology, 2020.
- [2] M. Dworkin, “Recommendation for block cipher modes of operation: Galois/Counter Mode (GCM) and GMAC”, NIST Special Publication 800-38D, National Institute of Standards and Technology, 2007.
- [3] P. W. Shor, “Algorithms for quantum computation: discrete logarithms and factoring”, in Proc. 35th Annual Symposium on Foundations of Computer Science, 1994, pp. 124–134.
- [4] S. Kent e K. Seo, “Security Architecture for the Internet Protocol”, RFC 4301, Internet Engineering Task Force, 2005.
- [5] S. Pirandola et al., “Advances in quantum cryptography”, Adv. Opt. Photon., vol. 12, pp. 1012–1236, 2020.
- [6] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus e M. Peev, “The security of practical quantum key distribution”, Rev. Mod. Phys., vol. 81, pp. 1301–1350, 2009.
- [7] H.-K. Lo, M. Curty e K. Tamaki, “Secure quantum key distribution”, Nat. Photon., vol. 8, pp. 595–604, 2014.
- [8] C. H. Bennett e G. Brassard, “Quantum cryptography: public key distribution and coin tossing”, in Proc. IEEE Int. Conf. Computers, Systems and Signal Processing, Bangalore, India, 1984, pp. 175–179.
- [9] H.-K. Lo, X. Ma e K. Chen, “Decoy state quantum key distribution”, Phys. Rev. Lett., vol. 94, 230504, 2005.
- [10] F. Grosshans e P. Grangier, “Continuous variable quantum cryptography using coherent states”, Phys. Rev. Lett., vol. 88, 057902, 2002.
- [11] H.-K. Lo, M. Curty e B. Qi, “Measurement-device-independent quantum key distribution”, Phys. Rev. Lett., vol. 108, 130503, 2012.
- [12] D. Stucki et al., “Fast and simple one-way quantum key distribution”, Appl. Phys. Lett., vol. 87, 194108, 2005.
- [13] ID Quantique, “IDQ unveils Cerberis XGR QKD Platform”, anúncio de produto, acesso em 27 jun 2026, <https://www.idquantique.com/idq-unveils-cerberis-xgr/>.
- [14] E. Dervisevic et al., “Quantum key distribution networks — key management: a survey”, ACM Comput. Surv., 2025.
- [15] ITU-T, “Y.3803: Quantum key distribution networks — key management”, International Telecommunication Union, 2020.
- [16] ETSI, “GS QKD 014: Quantum Key Distribution; Protocol and data format of REST-based key delivery API”, European Telecommunications Standards Institute.
- [17] FCMF, “Projeto INFREQUANT: iniciativa de pesquisadores do ITA é pioneira no campo da informação quântica”. Acesso em 27 jun 2026, <https://fcmf.org.br/projeto-infrequent-iniciativa-de-pesquisadores-do-ita-e-pioneira-no-campo-da-informacao-quantica/>
- [18] ETSI, “GS QKD 004: Quantum Key Distribution; Application interface”, European Telecommunications Standards Institute.
- [19] Força Aérea Brasileira, “DCTA é pioneiro no Brasil com criptografia quântica para atividades operacionais”, notícia institucional, 4 jun. 2026. Acesso em 27 jun. 2026, <https://www.fab.mil.br/noticias/ciencia-e-tecnologia/16915/2026/06/dcta-e-pioneiro-no-brasil-com-criptografia-quantica-para-atividades-operacionais/>
- [20] J. S. Buruaga et al., “The MadQCI cloud scenario: quantum as a service”, Entropy, vol. 28, no. 3, 283, 2026.
- [21] S. Fluhrer, P. Kampanakis, D. McGrew e V. Smyslov, “Mixing pre-shared keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for post-quantum security”, RFC 8784, IETF, 2020.
- [22] C. Kaufman, P. Hoffman, Y. Nir, P. Eronen e T. Kivinen, “Internet Key Exchange Protocol Version 2 (IKEv2)”, RFC 7296, Internet Engineering Task Force, 2014.
- [23] M. Takeoka, S. Guha e M. M. Wilde, “Fundamental rate-loss tradeoff for optical quantum key distribution”, Nat. Commun., vol. 5, 5235, 2014.
- [24] X. Gao et al., “IPSeQ: a security-enhanced IPsec protocol integrated with quantum key distribution”, IEEE Communications Magazine, 2025.
- [25] A. P. Lobo, “CPQD atinge distância de 200 quilômetros na transmissão de informações quânticas por fibra óptica”, Convergência Digital, 23 abr. 2026. Acesso em 27 jun 2026, <https://convergenciadigital.com.br/inovacao/cpqd-atinge-distancia-de-200-quilometros-na-transmissao-de-informacoes-quanticas-por-fibra-optica/>.
- [26] A. Tezzin, G. M. Uhdre, O. Martins, S. Rufo e V. G. A. Carneiro, “Long-term Performance Analysis of a Commercial QKD Device Under Real-world Deployment Conditions”, arXiv:2604.16236, 2026.
- [27] Commonwealth Scientific and Industrial Research Organisation (CSIRO), “Breakthrough quantum-secure link protects data using the laws of physics”, notícia institucional, 16 out. 2025. Acesso em 27 jun 2026, <https://www.csiro.au/en/news/All/News/2025/October/Breakthrough-quantum-secure-link-protects-data-using-the-laws-of-physics>
- [28] Y. Li et al., “Microsatellite-based real-time quantum key distribution”, Nature, vol. 640, pp. 47–54, 2025.
- [29] Stellenbosch University, “South Africa and China establish record-breaking 12,900 km ultra-secure quantum satellite link”, notícia institucional, 19 mar. 2025. Acesso em 27 jun 2026, <https://www.su.ac.za/en/node/19887>