Orquestração de Chaves Híbridas para Túneis IPsec

Esdras Silva[1], **Diego Abreu**[2], **Fernando Farias**[2], **Antônio Abelém**[1]

[1] Universidade Federal do Pará (UFPA)

[2]Rede Nacional de Ensino e Pesquisa (RNP)

antonio.vieira@icen.ufpa.br

{diego.abreu,fernando.farias}@rnp.br, abelem@ufpa.br

Resumo. *Ataques do tipo Harvest Now, Decrypt Later comprometem a confidencialidade de longo prazo das comunicações criptografadas. Como resposta, arquiteturas híbridas que combinam QKD e criptografia pós-quântica surgem como alternativa promissora, mas aumentam a demanda por entropia e a complexidade da gestão de chaves. Este trabalho analisa o impacto da rotação frequente de chaves híbridas em túneis IPsec, avaliando o equilíbrio entre segurança e consumo de entropia QKD. Os resultados mostram que rotações mais frequentes reduzem a exposição a ataques HNDL.*

Abstract. *Harvest Now, Decrypt Later attacks threaten the long-term confidentiality of encrypted communications. As a response, hybrid architectures combining QKD and post-quantum cryptography emerge as a promising alternative, but they increase entropy demand and key management complexity. This work analyzes the impact of frequent hybrid key rotation in IPsec tunnels, evaluating the trade-off between security and QKD entropy consumption. Results show that more frequent rotations reduce exposure to HNDL attacks .*

1. Introdução

A crescente ameaça de ataques do tipo *Harvest Now, Decrypt Later* (HNDL) tem impulsionado o desenvolvimento de mecanismos de proteção criptográfica capazes de garantir confidencialidade de longo prazo. Nesse contexto, a combinação de Distribuição de Chaves Quânticas (QKD) com criptografia pós-quântica (PQC) surge como uma abordagem promissora, permitindo a construção de esquemas híbridos com maior resiliência.

Trabalhos recentes têm explorado a integração de QKD com protocolos de rede tradicionais, como IPsec, demonstrando a viabilidade de orquestração contínua de chaves híbridas sem impacto significativo no desempenho do plano de dados . No entanto, ainda há lacunas na compreensão dos trade-offs entre políticas de rotação de chaves, consumo de entropia e exposição de dados.

Este trabalho propõe uma arquitetura de gerenciamento de chaves definida por software para túneis IPsec com chaves híbridas, aprofundando a análise em três dimensões complementares: (i) impacto do intervalo de rotação na exposição de dados e no desempenho, (ii) custo computacional intrínseco dos mecanismos pós-quânticos e (iii) influência da disponibilidade de entropia QKD na viabilidade operacional das políticas de rotação. As principais contribuições são a definição de um fluxo de orquestração para chaves híbridas, a avaliação experimental do trade-off entre rotação e consumo de entropia e

a análise de sustentabilidade em função da taxa efetiva de geração QKD. Os resultados, no cenário avaliado, indicam que rotações mais frequentes reduzem o volume de dados protegido por chave, sem impacto perceptível no throughput do túnel IPsec.

2. Fundamentação Teórica

A transição para cenários pós-quânticos introduz uma dimensão temporal na segurança criptográfica: dados cifrados hoje podem ser armazenados e decriptados no futuro com o avanço da computação quântica . Nesse contexto, a ameaça não se limita à capacidade atual do adversário, mas também à sua capacidade futura, tornando essencial considerar o ciclo de vida da informação e o tempo de adaptação dos sistemas.

No paradigma HNDL, o adversário intercepta e armazena comunicações cifradas para posterior decriptação [Lo et al. 2014]. Segundo o modelo temporal de Mosca [Mosca 2018], há vulnerabilidade quando o tempo de confidencialidade requerido (x) somado ao tempo de migração tecnológica (y) excede o horizonte estimado para quebra criptográfica (z), isto é, $x + y > z$. Essa relação evidencia que a segurança depende diretamente da rapidez na adoção de mecanismos resistentes e da redução da exposição das chaves ao longo do tempo. Nesse cenário, a Distribuição Quântica de Chaves surge como uma alternativa para geração de material criptográfico com segurança baseada em princípios físicos [Scarani et al. 2009]. Considerando uma taxa de geração R_{qkd} (bits/s), a quantidade de chave disponível em um intervalo t é dada por $K(t) = R_{qkd} \cdot t$. No entanto, essa disponibilidade é limitada e impõe restrições diretas sobre o uso das chaves no sistema.

Uma estratégia fundamental para mitigar riscos associados ao HNDL é a rotação frequente de chaves, conforme diretrizes clássicas de gerenciamento [Barker and Barker 2025]. Seja T_r o intervalo de rotação, com frequência $f_r = 1/T_r$. A redução de T_r diminui o volume de dados protegido por uma mesma chave, reduzindo a janela de exposição. Essa janela pode ser aproximada por $W_e \approx T_r + L_{rekey}$, onde L_{rekey} representa a latência associada ao processo de atualização das associações de segurança, incluindo handshake e sincronização entre os nós.

Entretanto, a rotação frequente aumenta o consumo de entropia. Se cada evento de rotação consome k bits, a taxa média de consumo é $C = k/T_r$. Para que o sistema opere de forma sustentável, é necessário garantir $C \leq R_{qkd}$, o que implica $T_r \geq k/R_{qkd}$. Esse limite explicita o trade-off central: intervalos menores aumentam a segurança temporal, mas podem exceder a capacidade de geração da infraestrutura QKD.

Dessa forma, a definição da política de rotação deve equilibrar três fatores principais: a exposição temporal das chaves, o custo operacional do rekey e a disponibilidade de entropia fornecida pela QKD. Esse modelo estabelece as bases teóricas que orientam a avaliação experimental apresentada na Seção 3.

3. Metodologia

A metodologia é guiada pelo modelo analítico da Seção 2 e avalia o impacto da rotação de chaves, da escolha de algoritmos pós-quânticos e da disponibilidade de entropia QKD. Os artefatos experimentais, incluindo scripts, configurações, métricas e rotinas de geração das figuras, estão disponíveis em repositório público[1].

[1] `https://github.com/ezrasilva/Wqnets-Orquestracao-Chaves-Hibridas-IPsec`

3.1. Arquitetura do sistema

A arquitetura experimental, ilustrada na Figura 1, segue um modelo de gerenciamento de chaves definido por software, no qual o plano de controle é separado do plano de dados. O sistema é composto por um orquestrador responsável pelo ciclo de vida das chaves, agentes de segurança executados nos gateways IPsec e um serviço QKD que fornece material criptográfico.

O orquestrador obtém entropia de nós QKD compatíveis com a interface ETSI e gera, de forma independente, um segredo compartilhado pós-quântico por meio de um mecanismo KEM da biblioteca libOQS[2]. No protótipo, a hibridização concatena o segredo pós-quântico ao material QKD e aplica HKDF-SHA256, produzindo uma chave simétrica híbrida de 32 bytes. Essa chave é então utilizada para atualizar as associações de segurança dos túneis IPsec via interface VICI do StrongSwan[3].

3.2. Rotação de chaves e configuração experimental

A rotação de chaves é coordenada pelo orquestrador e ocorre periodicamente com intervalo T_r. Em cada ciclo, o sistema obtém material do QKD, gera segredos PQC (via KEM), realiza a hibridização e distribui a nova chave aos gateways, que atualizam suas associações de segurança. Esse processo permite avaliar o impacto da frequência de rotação no desempenho e no consumo de entropia.

Os experimentos foram conduzidos com túneis IPsec entre dois gateways, sob tráfego contínuo. O plano QKD foi emulado com o QuKayDee[4], configurado com taxas de geração variáveis e expiração de 60 s. O intervalo de rotação T_r foi variado entre diferentes valores, e múltiplas execuções foram realizadas para cada configuração, permitindo a agregação dos resultados. Para avaliação da agilidade criptográfica, foi adotada uma abordagem complementar baseada em microbenchmarks de encapsulação e decapsulação dos algoritmos KEM. Essa escolha se deve à presença de uma latência dominante no processo de rekey, que mascara as diferenças entre os algoritmos quando analisados no sistema completo.

3.3. Métricas de avaliação

A avaliação considera o throughput do túnel IPsec, o consumo de entropia do QKD, o volume de dados protegido por chave e a latência do processo de rekey. Essas métricas permitem analisar o trade-off entre desempenho, uso de entropia e exposição de dados.

4. Resultados e Discussão

Esta seção analisa o impacto do intervalo de rotação de chaves T_r no desempenho do túnel IPsec, no consumo de entropia QKD e na viabilidade operacional do sistema. Os resultados são discutidos à luz do modelo analítico apresentado anteriormente. Os experimentos consideraram intervalos entre 2 s e 60 s, com 30 execuções por configuração.

4.1. Impacto da rotação de chaves

A Figura 2 apresenta o throughput do túnel e o consumo de entropia em função do intervalo de rotação T_r. Observa-se que o throughput permanece praticamente constante,

[2]**https://github.com/open-quantum-safe/liboqs**

[3]https://github.com/strongswan/strongswan

[4]https://qukaydee.com/pages/about

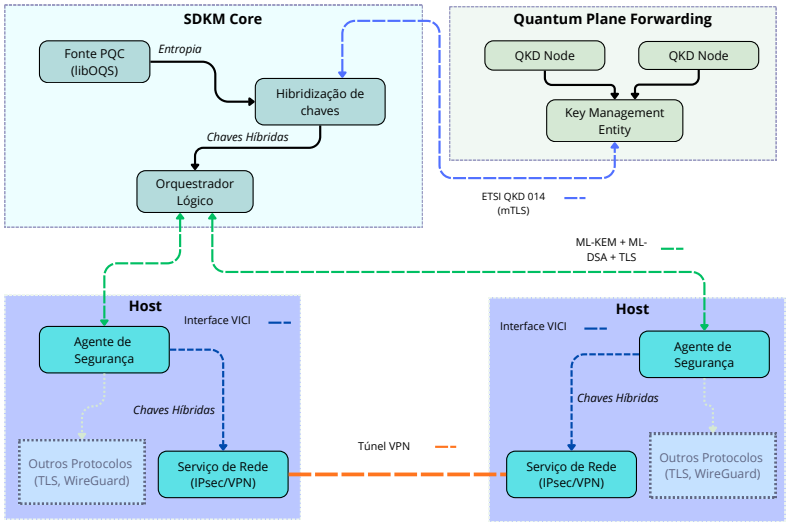

Figura 1. Arquitetura do sistema de orquestração de chaves híbridas utilizado na avaliação experimental.a

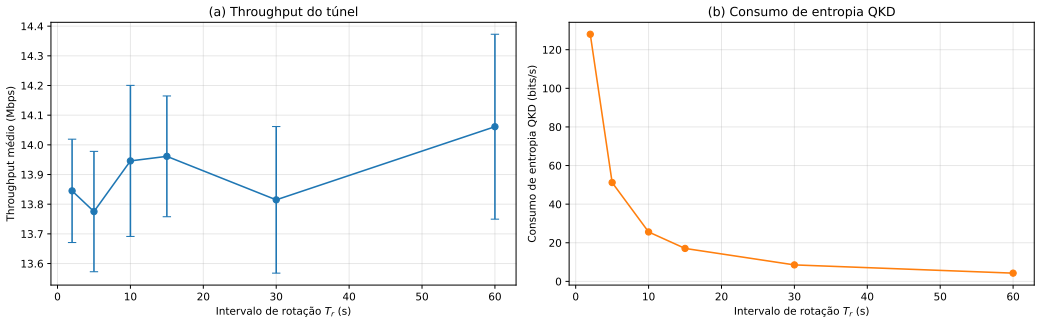

Figura 2. Impacto do intervalo de rotação de chaves T_r no throughput do túnel IPsec e no consumo de entropia do sistema QKD.

em torno de 14 Mbps, para todos os valores de T_r, indicando que o processo de rekey é transparente ao plano de dados.

Por outro lado, o consumo de entropia cresce significativamente com a redução de T_r, comportamento consistente com o modelo $C = k/T_r$. Assim, intervalos menores aumentam a demanda por material criptográfico QKD.

Considerando o throughput estável, o volume de dados protegido por chave cresce linearmente com T_r. Por exemplo, para 14 Mbps, $T_r = 60$ s resulta em cerca de 840 Mbits por chave, enquanto $T_r = 2$ s reduz esse valor para aproximadamente 28 Mbits. Esses resultados evidenciam um trade-off fundamental: intervalos menores reduzem a exposição de dados, mas aumentam o consumo de entropia.

4.2. Agilidade criptográfica

A segunda bateria de experimentos avaliou o impacto da escolha do algoritmo PQC no processo de estabelecimento de chaves, mantendo constantes os demais parâmetros do sistema. A Figura 3 apresenta os resultados do microbenchmark dos algoritmos PQC avaliados.

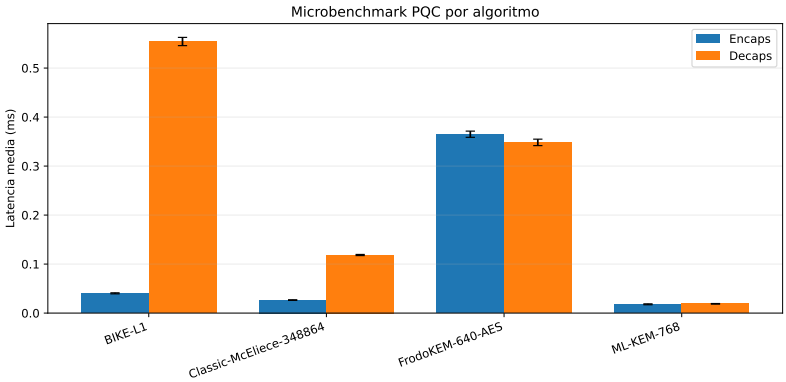

Figura 3. Resultados da avaliação de agilidade criptográfica: encapsulação e decapsulação variados entre os algoritmos KEM.

Observa-se variação no custo de encapsulação e decapsulação entre os algoritmos, refletindo diferenças em suas construções criptográficas. No entanto, essas diferenças não produziram impacto perceptível no throughput do túnel, indicando que a arquitetura desacopla o custo criptográfico do plano de dados e permite a substituição de mecanismos pós-quânticos sem degradação relevante no cenário avaliado.

4.3. Sustentabilidade da entropia QKD

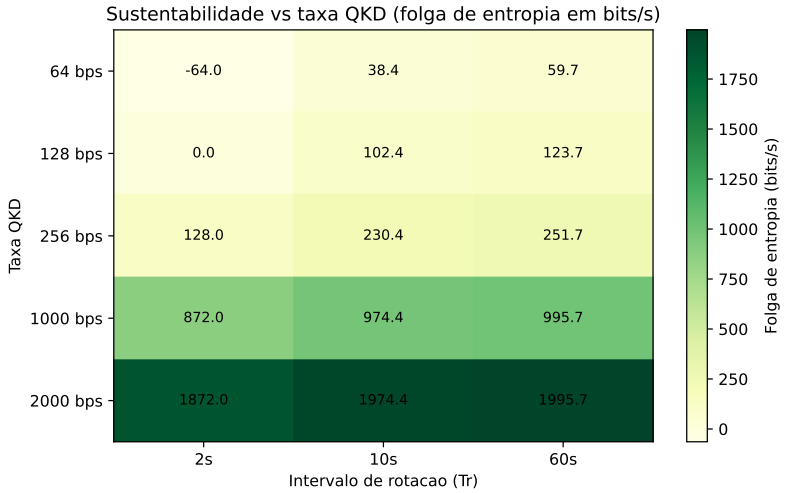

Figura 4. Avaliação de Sustentabilidade da entropia QKD.

A Figura 4 apresenta a relação entre a taxa de geração QKD R_{qkd}, o intervalo de rotação T_r e a folga de entropia do sistema. Os resultados mostram que a viabilidade da rotação de chaves é diretamente limitada pela capacidade de geração de entropia do sistema QKD. Para combinações de R_{qkd} e T_r em que o consumo excede a geração, observa-se folga negativa, caracterizando uma região operacional inviável.

Em particular, para taxas reduzidas de QKD e intervalos agressivos de rotação, o sistema torna-se insustentável, pois a demanda por chaves supera a capacidade de geração. Por outro lado, para valores maiores de R_{qkd} ou intervalos mais longos de T_r, o sistema opera com folga positiva, indicando estabilidade operacional.

Os resultados permitem identificar uma condição prática de operação, na qual o sistema deve satisfazer $T_r \geq k/R_{qkd}$ para garantir sustentabilidade. Além disso, observa-se a existência de pontos limiares em que o sistema opera próximo do limite de sua capacidade, caracterizando regiões críticas de operação.

Esses resultados corroboram o modelo analítico e indicam que a definição de políticas de rotação deve considerar explicitamente as limitações da infraestrutura QKD. Como limitação, o modelo adotado abstrai a taxa QKD por uma taxa efetiva média e não contempla variações temporais de geração, múltiplos túneis concorrentes ou falhas prolongadas do serviço QKD.

5. Conclusão

Este trabalho investigou a orquestração de chaves híbridas em túneis IPsec, avaliando o impacto da rotação periódica sobre desempenho, consumo de entropia e exposição de dados. No cenário experimental avaliado, os resultados indicam que rotações mais frequentes reduzem o volume de dados protegido por chave sem impacto perceptível no throughput do túnel. Por outro lado, a redução do intervalo de rotação aumenta o consumo de entropia QKD, evidenciando um trade-off entre segurança temporal e disponibilidade de material criptográfico. A viabilidade operacional depende da relação entre o intervalo de rotação, o consumo por evento de rekey e a taxa efetiva de geração QKD. Como trabalhos futuros, pretende-se avaliar múltiplos túneis concorrentes, taxas QKD variáveis e políticas adaptativas de rotação.

Agradecimentos

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

Referências

Barker, E. and Barker, W. C. (2025). Recommendation for key management: Part 1 – general. Technical Report NIST Special Publication 800-57 Part 1 Rev. 5 (Upd. 1), National Institute of Standards and Technology (NIST).

Lo, H.-K., Curty, M., and Tamaki, K. (2014). Secure quantum key distribution. *Nature Photonics*, 8(8):595–604.

Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy*, 16(5):38–41.

Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., and Peev, M. (2009). The security of practical quantum key distribution. *Reviews of Modern Physics*, 81(3):1301–1350.