Estratégias Preliminares de Consumo de Chaves Quânticas na Rede Hermes Quântica

João Alfredo Bessa [1], Alisson Tezzin [2], Gustavo Udhre [2], Oscar Martins [2], Rosiane de Freitas[1], Vítor G. Andrezo C. [2]

[1]Instituto de Computação – Universidade Federal do Amazonas, Manaus, Brasil.

[2]Seção de Engenharia de Defesa – Instituto Militar de Engenharia, Rio de Janeiro, Brasil.

{joao.bessa,rosiane}@icomp.ufam.edu.br
{alisson.cordeiro,gustavo.uhdre,martins.oscar,andrezo}@ime.eb.br

Abstract. *The advancement of quantum computing poses a significant threat to classical asymmetric cryptographic algorithms, such as RSA and ECC, due to their vulnerability to Shor's algorithm. In response, Quantum Key Distribution (QKD) has emerged as a robust solution, leveraging the laws of quantum physics to ensure secure key exchange. This paper presents the current infrastructure and preliminary key consumption strategy of the Hermes Quantum Network (RHQ). The network implements the BB84 protocol with time-bin phase encoding. The proposed communication strategy employs a peer-to-peer (P2P) secure channel using AES-256 GCM authenticated encryption, where cryptographic keys are dynamically consumed from a key bank.*

Resumo. *O avanço da computação quântica representa uma ameaça significativa aos algoritmos criptográficos assimétricos clássicos, como RSA e ECC, devido à sua vulnerabilidade ao algoritmo de Shor. Em resposta, a Distribuição Quântica de Chaves (QKD) surgiu como uma solução robusta, aproveitando as leis da física quântica para garantir a troca segura de chaves. Este artigo apresenta a infraestrutura atual e a estratégia preliminar de consumo de chaves da Rede Quântica Hermes (RHQ). A rede implementa o protocolo BB84 com codificação de fase por intervalos de tempo. A estratégia de comunicação proposta emprega um canal seguro ponto a ponto (P2P) utilizando criptografia autenticada AES-256 GCM, onde as chaves criptográficas são consumidas dinamicamente a partir de um banco de chaves.*

1. Introdução

A segurança dos algoritmos assimétricos clássicos repousa na intratabilidade de problemas matemáticos específicos para computadores convencionais. No entanto, com o avanço da computação quântica, o algoritmo de Shor demonstrou teoricamente a capacidade de fatorar inteiros e resolver logaritmos discretos em tempo polinomial, comprometendo esquemas como RSA e ECC [Shor 1994]. Em contrapartida, os algoritmos simétricos como o AES são significativamente mais resilientes. Embora o algoritmo de Grover reduza o espaço de busca de chaves à sua raiz quadrada efetiva, a adoção de chaves de 256 bits (como o AES-256) mantém um nível de segurança adequado contra ataques quânticos de força bruta [Grover 1996].

Esse cenário motiva uma transição global para novos métodos de segurança. Além da busca pela Criptografia Pós-Quântica (PQC), ganha força a adoção de protocolos de Distribuição Quântica de Chaves (QKD). Esses protocolos permitem a geração e distribuição de chaves simétricas apoiadas nas leis fundamentais da física quântica, garantindo o abastecimento seguro de chaves para cifras, como o AES-GCM *(Advanced Encryption Standard - Galois/Counter Mode)*, e tornando o canal imune a avanços computacionais futuros. Assim, este trabalho apresenta a configuração atual da Rede Hermes Quântica e sua estratégia inicial de consumo de chaves.

2. Infraestrutura da Rede Hermes Quântica

A Rede Hermes Quântica (RHQ) é uma iniciativa do Instituto Militar de Engenharia (IME), focada em criar uma rede metropolitana de comunicação quântica voltada para a defesa. A etapa atual visa interligar o IME a outra iniciativa, chamada Rede Rio Quântica, por meio de um enlace QKD com o Centro Brasileiro de Pesquisas Físicas (CBPF).

Na configuração atual, a rede usa um equipamento da empresa suíça ID Quantique, chamado Clavis [Xu et al. 2023], um sistema QKD de quarta geração que opera o protocolo BB84 com estados de isca (*decoy states*). Sua codificação é baseada em fase e tempo *(time-bin phase encoding)* [Vagniluca et al. 2020]. A plataforma é estruturada em uma arquitetura de ”caixa cinza”, que permite a análise de dados brutos em múltiplos estágios da destilação de chaves (pós-processamento), além de oferecer controle de parâmetros de hardware, como níveis de atenuação e temporização de portas. Nesta fase preliminar, a extração foi feita no estágio final da destilação das chaves, após a amplificação de privacidade e expansão das chaves. Um enlace real de cerca de 3,5 km de fibra óptica está sendo usado para conectar o emissor (Alice) ao receptor (Bob).

3. Estratégia de Comunicação e Consumo de Chaves

A estratégia de comunicação estabelece um canal seguro *peer-to-peer* com criptografia simétrica autenticada (AES-GCM), consumindo chaves de um banco, de forma dinâmica e contínua. O esquema geral pode ser visualizado na Figura **1**.

3.1. Inicialização e Derivação de Chaves

Os sistemas Clavis operam na camada física gerando chaves criptográficas simétricas quanticamente seguras através de links ópticos, as quais são repassadas e armazenadas continuamente em seus respectivos Sistemas de Gerenciamento de Chaves (KMS). O algoritmo consumidor atua na camada de aplicação, interagindo com esses módulos via API REST ETSI014. Esse algoritmo roda nas duas pontas, requisita as chaves e as armazena em um banco de chaves espelho. Ao iniciar, os nós acessam o banco de chaves e carregam na memória RAM o mapeamento de `KeyID` para o respectivo valor da chave.

3.2. Fluxo de Envio (Consumo e Criptografia)

Quando uma mensagem é inserida, o sistema verifica se há chaves disponíveis na memória. Se o dicionário estiver vazio, uma nova leitura do banco de chaves é disparada automaticamente. O nó seleciona a primeira chave disponível e separa seu `KeyID`. Um *nonce* (vetor de inicialização) criptograficamente seguro de 12 *bytes* é gerado aleatoriamente pelo sistema operacional. A mensagem é cifrada via AES-GCM, garantindo

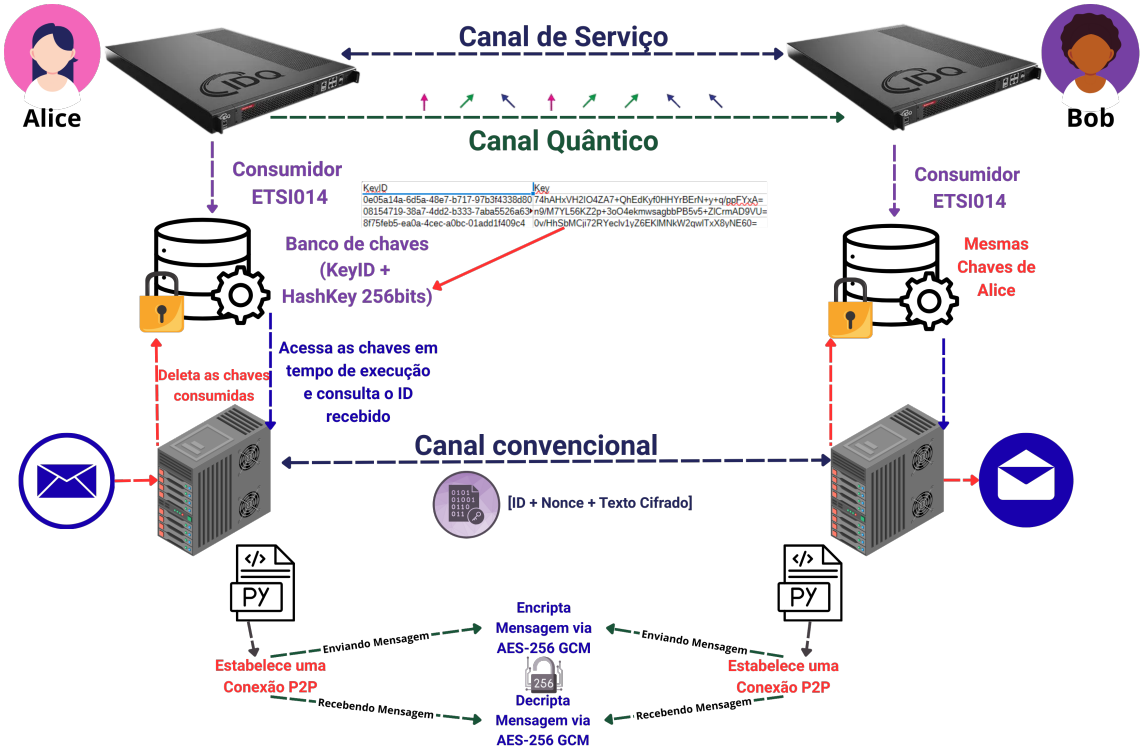

Figura 1. Esquema geral da comunicação criptografada na RHQ.

confidencialidade e gerando uma *tag* de autenticação embutida (para integridade). O *payload* enviado pelo *socket* possui a estrutura exata: `[KeyID] + [\n] + [Nonce] + [Texto Cifrado]`. Após o envio, a chave é deletada da memória do remetente, aplicando uma política de *uso único da chave* (*one-time key*). Ressalta-se que o esquema preserva a segurança computacional do AES-256-GCM e não confere a segurança incondicional do *One-Time Pad*, dado que a cifragem não opera com chave do tamanho da mensagem.

3.3. Fluxo de Recebimento (Sincronização e Decriptografia)

Uma *thread* dedicada roda em *background* para receber pacotes sem bloquear a interface de envio. O pacote recebido é fatiado no delimitador `\n` para isolar o `KeyID`. Os primeiros 12 *bytes* do restante da carga formam o *nonce*, e o resto compõe o texto cifrado. Se o receptor não encontrar o `KeyID` em sua memória local (indicando que sua lista de chaves está defasada), ele realiza um novo *fetch* no banco de chaves. A mensagem é decriptada e sua integridade é validada simultaneamente pelo AES-GCM. A chave utilizada é imediatamente deletada do banco e da memória do receptor. O sistema assume que um processo externo e paralelo de distribuição quântica é responsável por popular o banco de chaves físico subjacente conforme o consumo avança, garantindo que novas chaves sejam carregadas quando o estoque atual se esgotar.

4. Resultados dos Consumidores Implementados

A Figura **2** mostra a execução dos dois consumidores (Alice e Bob) e sua interação direta na troca de mensagens. Para investigar os desafios seguintes, foram realizados testes

preliminares em ambiente *simulado* (Mininet) com chaves pré-geradas extraídas dos consumidores; a Figura **3** apresenta os tempos observados. Tais valores refletem o ambiente de simulação e não devem ser interpretados como latências do enlace QKD real — a caracterização do enlace físico fica como passo subsequente.

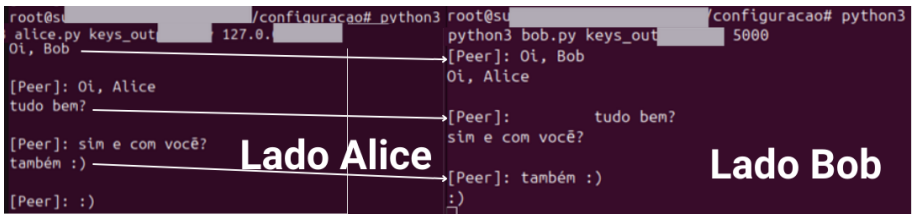

Figura 2. Execução dos consumidores em troca de mensagens via P2P.

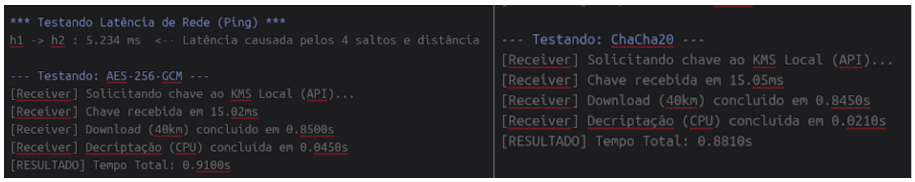

Figura 3. Tempos observados em simulação (Mininet) de enlace de 40 km com 4 nós, comparando AES-256-GCM e ChaCha20.

Na configuração atual, o sistema Clavis fornece cerca de 10.000 chaves por hora ao KMS, suficiente para a troca demonstrada. Sob cargas mais elevadas, a taxa de geração tende a se tornar gargalo; como trabalhos futuros, pretende-se investigar mecanismos de expansão de chaves, políticas de *rekeying* adaptativo, a caracterização dos componentes de latência no enlace QKD real e métricas de escalabilidade e sincronização do consumo em cenários com múltiplos nós e tráfego concorrente.

Agradecimentos

Os autores gostariam de agradecer à FINEP pelo apoio financeiro por meio do Projeto FINEP/MCTI nº 3310/24 – Pesquisa e Desenvolvimento de Tecnologias Quânticas para Segurança e Defesa Nacional (Quantum II). Este trabalho também é parcialmente apoiado pelas agências CAPES PROEX - Financiamento Código 001, CNPq e FAPEAM.

Referências

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219.

Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134. IEEE.

Vagniluca, I., Da Lio, B., Rusca, D., Cozzolino, D., Ding, Y., Zbinden, H., Zavatta, A., Oxenløwe, L. K., and Bacco, D. (2020). Efficient time-bin encoding for practical high-dimensional quantum key distribution. *Physical Review Applied*, 14(1):014051.

Xu, G., Mao, J., Sakk, E., and Wang, S. P. (2023). An overview of quantum-safe approaches: quantum key distribution and post-quantum cryptography. In *2023 57th Annual Conference on Information Sciences and Systems (CISS)*, pages 1–6. IEEE.