Propostas de Projetos de Pesquisa 2026

Prof. Dr. Gabriel Dias Carvalho[†]

1. Proposta para Pesquisa e Desenvolvimento

Revisão e Avanços em Protocolos de Comunicação e Criptografia Quânticas, com Integração de Criptografia Pós-Quântica

Esta pesquisa propõe uma abordagem sobre os avanços em comunicação e criptografia quânticas, com ênfase na revisão crítica da literatura especializada e no desenvolvimento de melhorias de protocolos existentes, como o BB84 e variantes [1]. Além disso, busca integrar essas tecnologias com sistemas de criptografia pós-quântica, criando soluções híbridas que atendam às demandas de segurança diante do avanço iminente da computação quântica. Os objetivos principais incluem realizar uma revisão sistemática e crítica dos principais protocolos de distribuição quântica de chaves (QKD), abordando sua segurança, eficiência e limitações, com destaque para aspectos como ruído quântico e ataques adversos [2, 3]. Também visa investigar algoritmos de correção de erros e novas abordagens para mitigar a descoerência [4]. E melhorar a resiliência dos protocolos em cenários práticos, explorando a integração de QKD com criptografia pós-quântica [5] para combinar a segurança física dos sistemas quânticos com a robustez matemática dos algoritmos resistentes a ataques quânticos.

A pesquisa será conduzida em três etapas principais. Na primeira etapa, será realizada uma revisão de literatura especializada, analisando detalhadamente os protocolos QKD existentes, dos BB84 e E91 [6] aos mais modernos [1], abordando implementações baseadas em variáveis discretas e contínuas, além das limitações práticas, como alcance, taxa de erro e vulnerabilidades a ataques. Também serão revisados os desafios tecnológicos para implementação, incluindo o uso de repetidores quânticos e canais de comunicação híbridos [2, 3]. Na segunda etapa, serão exploradas e desenvolvidas melhorias nos protocolos, com foco no estudo de algoritmos para correção de erros quânticos e mitigação de problemas de descoerência e ruído. Pretendo propor soluções para integrar QKD em infraestruturas clássicas, utilizando gateways especializados para comunicação entre sistemas quânticos e clássicos, além do desenvolvimento de simulações computacionais para avaliar o desempenho e viabilidade, empregando ferramentas como NetSquid [7]. Por fim, na terceira etapa, será explorada a integração com criptografia pós-quântica, avaliando algoritmos por exemplo do tipo Lattice-Based Cryptography e Multivariate Cryptography [5], com o objetivo de propor soluções híbridas que combinem a distribuição quântica de chaves com algoritmos pós-quânticos, fortalecendo a segurança.

A possibilidade de impacto desta pesquisa está na criação de base tecnológica sólida para sistemas de comunicação seguros e escaláveis, com aplicações em redes de IoT críticas, incluindo dispositivos médicos e automação industrial e infraestruturas que demandem alta segurança, além de redes de transporte inteligente, como veículos autônomos. O desenvolvimento de soluções híbridas também contribuirá para a transição segura para a era pós-quântica, fortalecendo a independência tecnológica e a soberania nacional em segurança cibernética.

[†] gdc@poli.br.

2. Propostas de Projetos de Pesquisa

Proposta 1: **Desenvolvimento de Protocolos Resilientes de QKD e Integração com Criptografia Pós-Quântica**

Breve descrição: Esta proposta busca revisar os principais protocolos de distribuição quântica de chaves (QKD), dos mais antigos, como o BB84 [8], aos mais recentes [1] e explorar melhorias viáveis com foco em sua resiliência contra ruído quântico e ataques adversos. A pesquisa envolverá o estudo de novos algoritmos de correção de erros além de estratégias para integrar tais protocolos com métodos de criptografia pós-quântica [5]. A abordagem híbrida visa combinar a segurança física dos sistemas quânticos com a robustez matemática dos algoritmos resistentes à computação quântica, garantindo soluções completas para cenários de comunicação segura. Com potencial aplicação em redes seguras de comunicação para proteção de dados, esta integração se torna estratégica diante da possibilidade de computadores quânticos capazes de quebrar sistemas criptográficos clássicos.

Proposta 2: **Integração de Protocolos Quânticos em Infraestruturas Clássicas**

Breve descrição: A proposta visa investigar a integração de protocolos de comunicação quântica em infraestruturas clássicas, criando redes híbridas que combinem a segurança quântica com a flexibilidade clássica. Serão analisados desafios técnicos como a compatibilidade entre dispositivos quânticos e clássicos, utilizando gateways e interfaces específicas, além de explorar métodos para gerenciar recursos e autenticação, integrando a distribuição quântica de chaves (QKD) com sistemas clássicos. A pesquisa abordará também a resiliência e escalabilidade, desenvolvendo soluções como repetidores quânticos para superar limitações de alcance e descoerência. Aplicações práticas incluem a proteção de dados em redes de IoT e a segurança de comunicações em transportes inteligentes. Simulações e testes experimentais poderão validar os protocolos híbridos, avaliando desempenho e viabilidade em diferentes cenários.

3. Referências

[1] Kumar, A., Garhwal, S. ”State-of-the-art survey of quantum cryptography.” Archives of Computational Methods in Engineering, 28(5), 3831-3868 (2021).

[2] S. Pirandola, et al. ”Advances in quantum cryptography,” Adv. Opt. Photon., 12, 1012-1236 (2020).

[3] Gisin, N., et al. ”Quantum cryptography.” Reviews of Modern Physics, 74(1), 145 (2002).

[4] Schlosshauer, M. ”Quantum decoherence.” Physics Reports, 831 (2019).

[5] Bernstein, D., and Lange, T. ”Post-quantum cryptography.” Nature, 549, 188–194 (2017).

[6] Ekert, A.K. ”Quantum cryptography based on Bell’s theorem.” Physical Review Letters, 67, 661-663 (1991).

[7] https://netsquid.org.

[8] Bennett, C. H., Brassard, G., ”Quantum cryptography: Public key distribution and coin tossing.” Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing (1984).