JORNADA PCI
APRESENTAÇÃO DE PROJETO – 2021/2022

BOLSISTA: MÁRCUS ANDRÉ GOMES BARBOSA
SUPERVISOR: NILTON ALVES JÚNIOR
MODALIDADE: PCI-DD

REDERIO QUÂNTICA

OBJETIVO

Implementar uma rede de comunicação quântica conectando as instituições **CBPF**, **UFF**, **PUC**, **UFRJ** e **IME** a partir do canal clássico de comunicação, estruturado pelas fibras óticas da **Rede-Rio/RedeCOMEPRio**, já existente entre estas instituições. Inicialmente, pretende-se estabelecer as condições básicas necessárias que possibilitem a implementações de diversos protocolos de comunicação quântica, abrindo caminho para a integração do Brasil à Internet Quântica.

INTRODUÇÃO

Criptografia clássica

CRIPTOGRAFIA: CHAVE + ALGORÍTMO

ONE TIME PAD (OTP)

Criptografia Simétrica
Chave única (privada)

Criptografia Assimétrica
Chave pública e privada

Figura 1: Esquema de chave simétrica e assimétrica.

LIMITES

- Criptografia baseada na fatoração de números primos muito grandes;
- Transmissão de chaves via canal público;
- A segurança depende somente da capacidade computacional, não é uma questão físico-matemática.

Criptografia quântica

PRINCÍPIOS DA MECÂNICA QUÂNTICA

- Superposição de estados;
- Perturbação (colapso) do sistema quântico ao se realizar uma medida;
- Princípio de Heisenberg;
- Não clonagem.

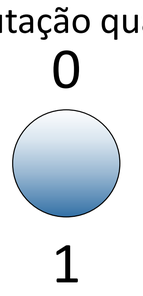
CLÁSSICO X QUÂNTICO

Bit
(computação clássica)

0

1

Qubit
(computação quântica)



QKD NA PRÁTICA

PROTOCOLOS QKD
(DISTRIBUIÇÃO QUÂNTICA DE CHAVES)

QKD COM 1 FÓTON

- BB84

QKD COM 2 FÓTONS

- Emaranhamento

MDI-QKD

TWIN FIELDS

REPETIDORES QUÂNTICOS

ATIVIDADES REALIZADAS

Visibilidade para enlace aéreo

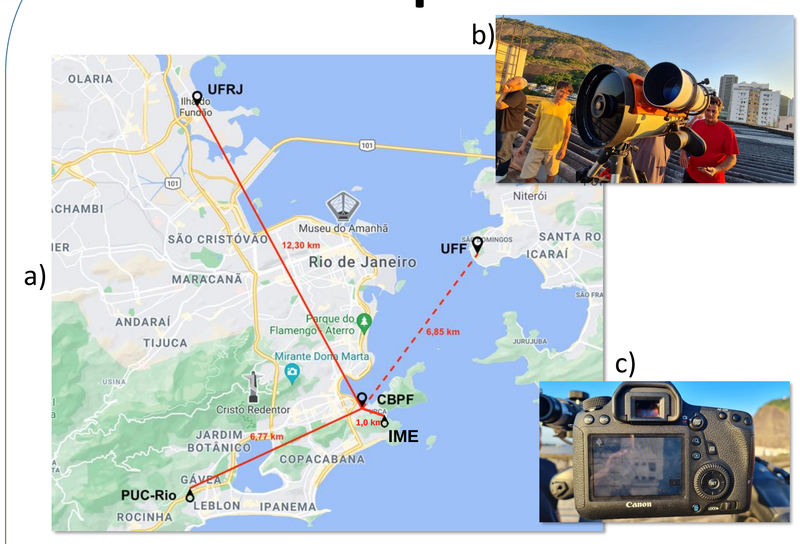


Figura 2: a) Mapa com localização das instituições. b) Telescópio utilizado para observação da UFF. c) Câmera acoplada ao telescópio.

Teste de estabilidade – PUC

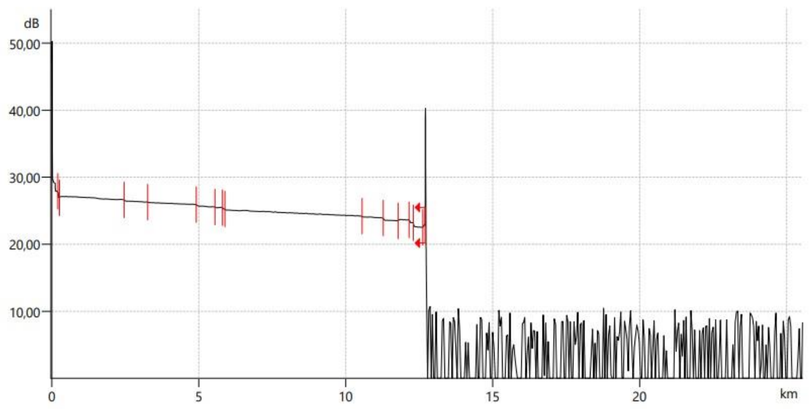


Figura 3: Gráfico da relação dB x km.

PRÓXIMOS PASSOS

- Aquisição da aparelhagem básica para testes de envio e recebimento de fótons polarizados em pequenas distâncias;
- Caracterização e estabilização do canal quântico;
- Implementação e testes de protocolos e algoritmos de sinalização, MDI-QKD

MOTIVAÇÃO

Illinois Express Quantum Network for Distributing and Controlling Entanglement on Metro-Scale (2021).

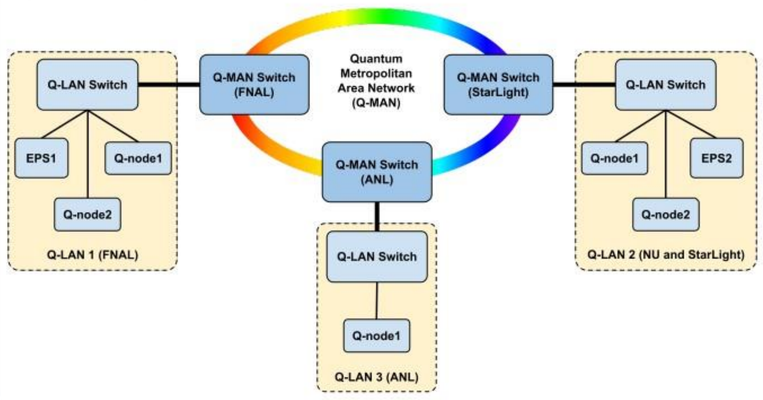


Figura 4: Topologia IEQNET.

REFERÊNCIAS

COHEN, F. **A short history of cryptografy**, 1995. GISIN, N. et al. **Quantum Cryptography**, 2022. RIGOLIN, G.; RIEZNIK, A. A. **Introdução à criptografia quântica**, 2005. WU, W. et al. **Illinois Express Quantum Network for Distributing and Controlling Entenglement on Metro-Scale**, 2021.

AGRADECIMENTOS

CBPF Centro Brasileiro de Pesquisas Físicas
CNPq Conselho Nacional de Desenvolvimento Científico e Tecnológico