GERCOM

Estudo e Simulação de uma Rede de Distribuição de **Chaves Quânticas de Alto Desempenho para o Campus da UFPA**

Autores:

David Tavares[1], Arthur Pimentel[1], Diego Abreu[12], Antônio Abelém[12]

1 UNIVERSIDADE FEDERAL DO PARÁ (UFPA)
[2]PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO (PPGCC)

Agenda

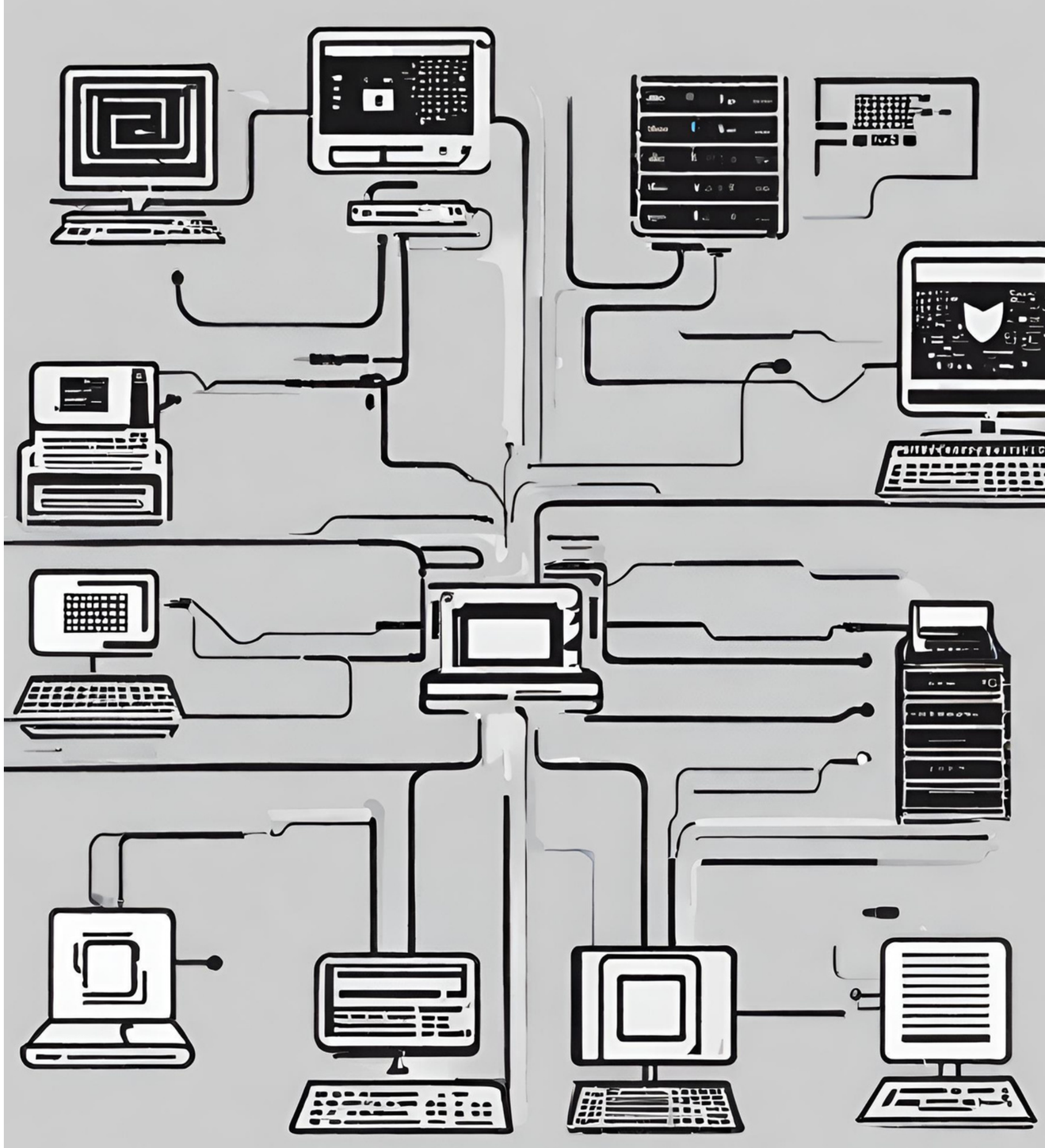
1. Objetivo
2. Segurança Atual
3. Computação e Comunicação Quântica
4. Distribuição de Chaves Quânticas
4. Experimento e Metodologia
4. Resultados
5. Trabalhos Futuros e Agradecimentos

Objetivo

O objetivo deste artigo é apresentar um projeto de uma rede QKD personalizada, para atender ás demandas especificas do campus da Universidade Federal do Para (UFPA)

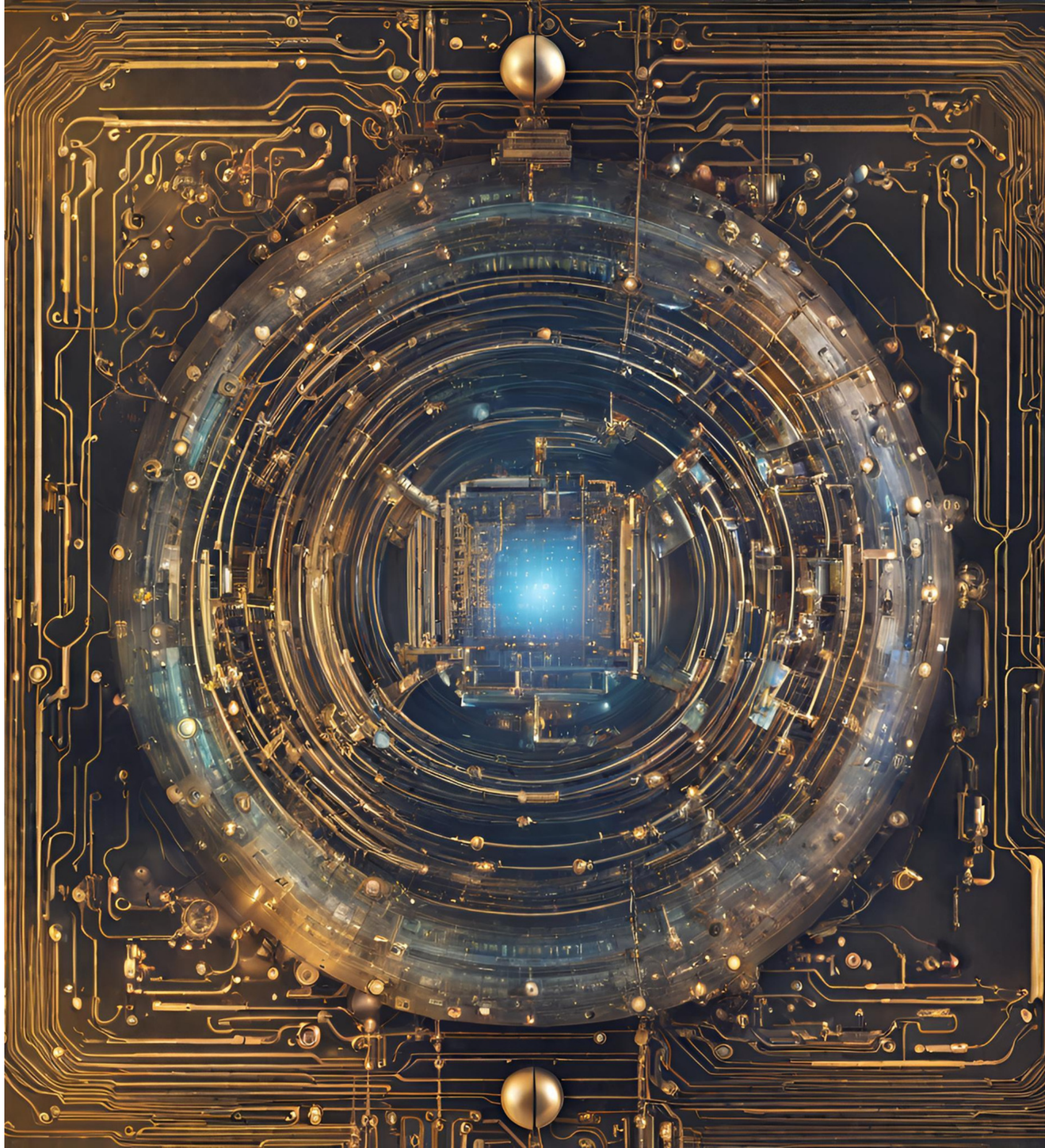
Segurança Atual

- Principais desafios
- Criptografia de chaves públicas
- Chaves pública e privada
- Chave pública
- Chave privada



Computação Quântica

- Qubit
- Superposição e Entrelaçamento
- Aplicação

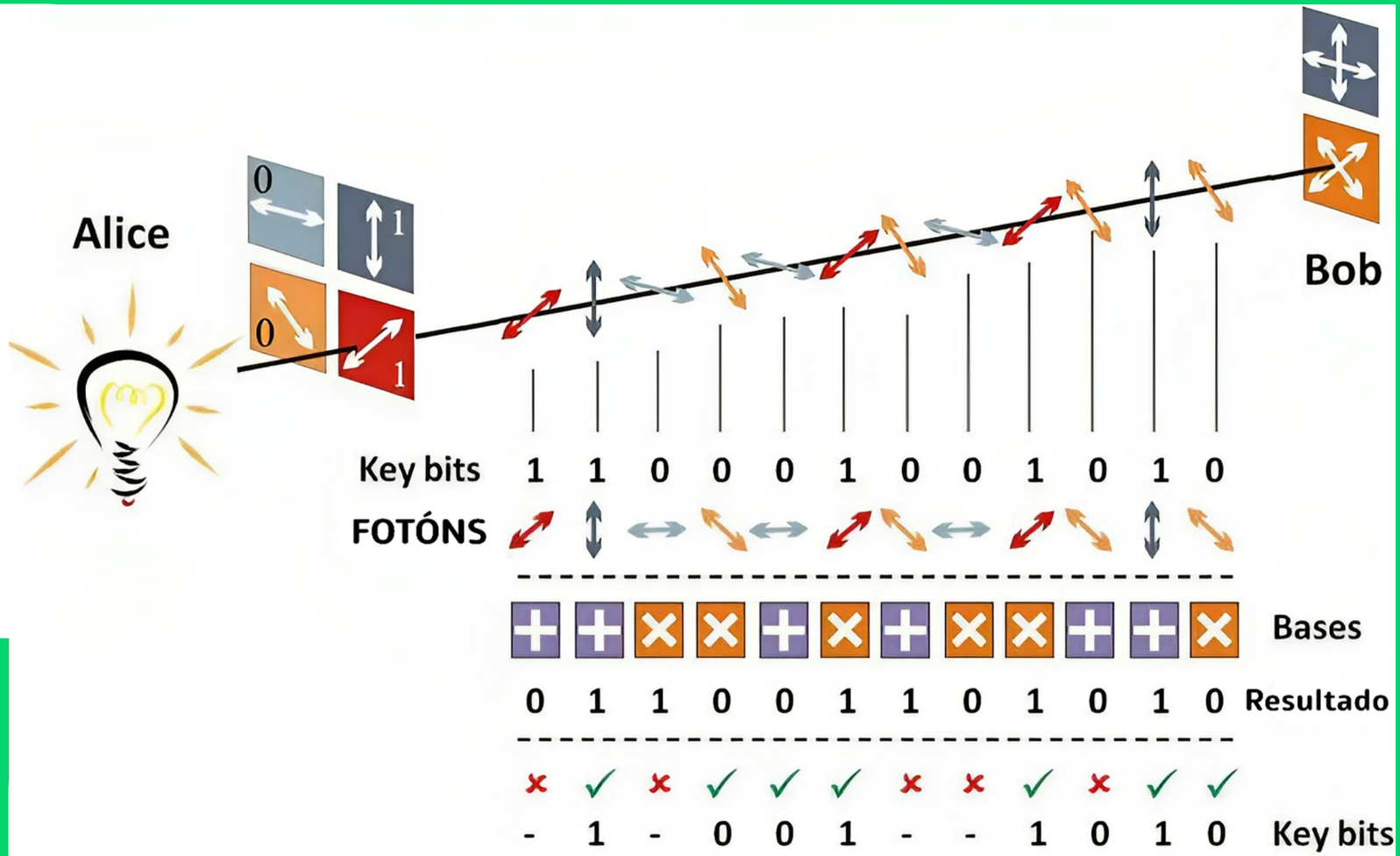


Comunicação Quântica

- processo de teletransporte
- Impossibilidade de cópia não detectada
- Segurança garantida a nível de rede
- Interceptação monitorável

Distribuição Quântica de Chaves

Protocolo BB84



Detalhe

Alice e Bob estão conectados por um canal quântico

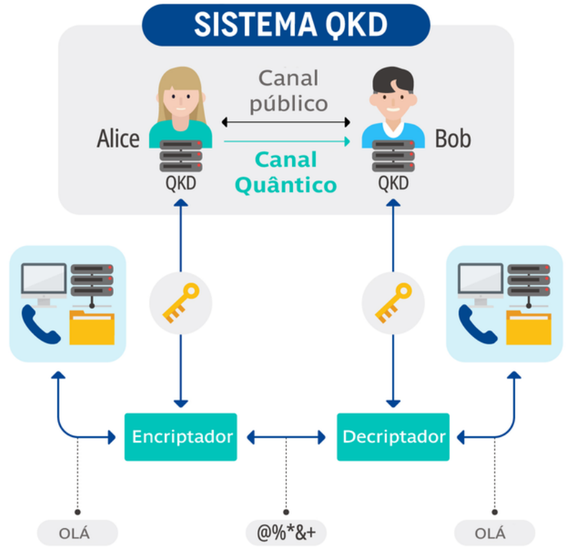
Detalhe 2

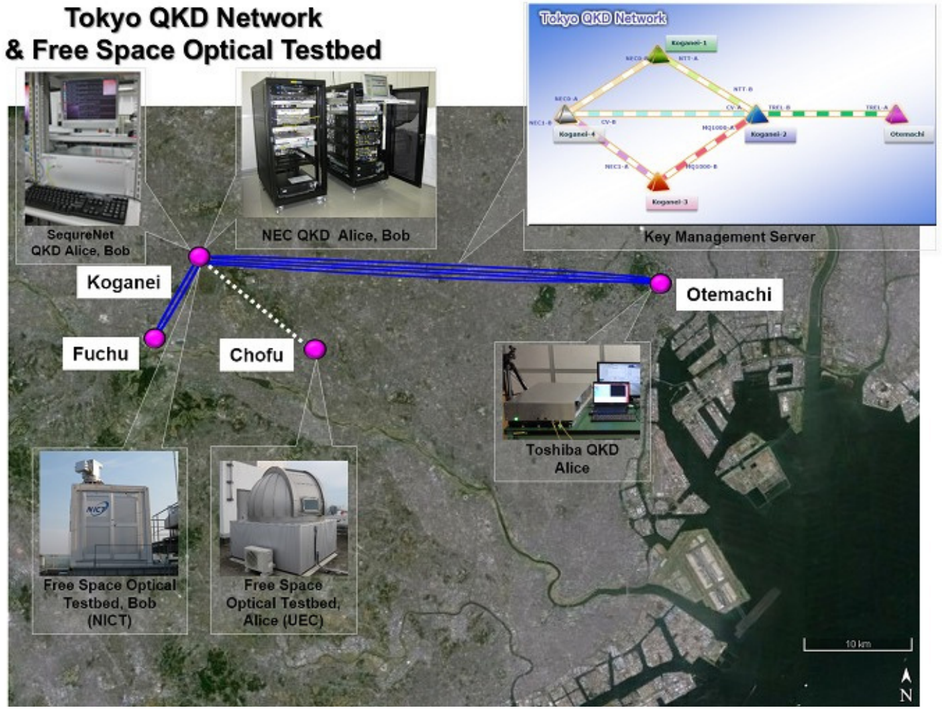
Alice envia os fótons para Bob.

Detalhe 3

Alice e Bob comunicam suas bases para cada fóton

Rede de distribuição de chaves quânticas (QKD)





Alice:

O nó de distribuição de chaves. Alice é responsável por gerar e transmitir estados quânticos para Bob

Bob:

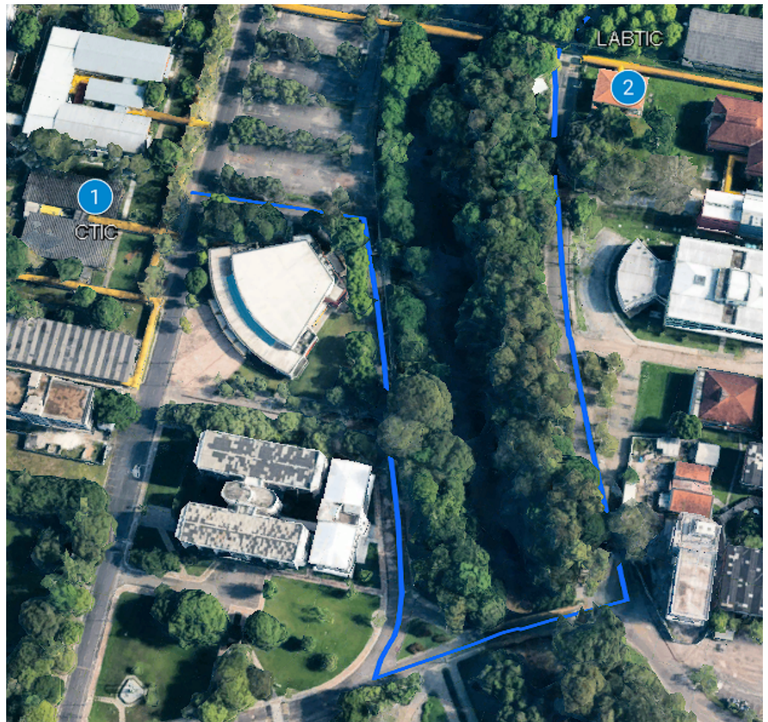
O nó de medição. Bob é responsável por medir estados quânticos recebidos de Alice

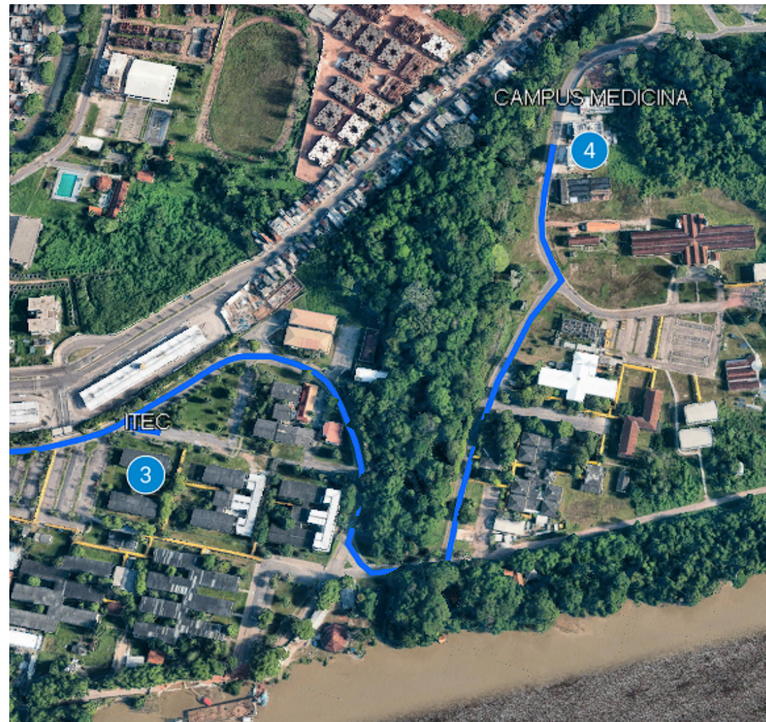
Canal Quântico:

O meio de transmissão que permite a propagação de estados quânticos de Alice para Bob

Experimento e Metodologia

- Simulador OpenKQD
  - Projeto da União Europeia
  - Dados de equipamentos reais
- Campus UFPA
- 4 nós
- Mais de 2KM





Tabelas de Experimentos

- KeyRate: Quantidade de bits de chave segura geradas
  - KeyRate Calculado
- Keysize: Total de bits na chave segura
- Apprate: Quantidade de dados que podem ser criptografados
- KDU: Quantos dados precisam ser transmitidos para gerar uma chave segura.
- MC: Pacotes perdidos
- VMAC: autenticação de mensagem que é usado para verificar a integridade
- OTP: Senha de único uso

Configurações do Experimento.

QKD link	Distância	KeyRate Calculada	KeySize	AppRate
Link 1-2	591 (m)	1463 (kbps)	10 kb	20Kb/s
Link 2-3	498 (m)	1736 (kbps)	10 kb	20Kb/s
Link 3-4	945 (m)	915 (kbps)	10kb	20Kb/s

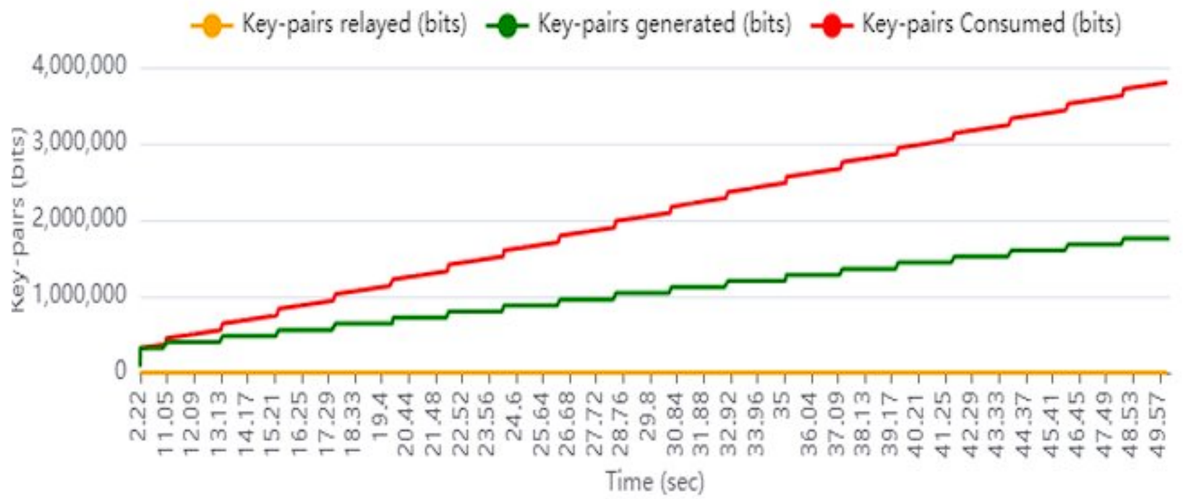
Resultados dos Experimento para rede QKD UFPA.

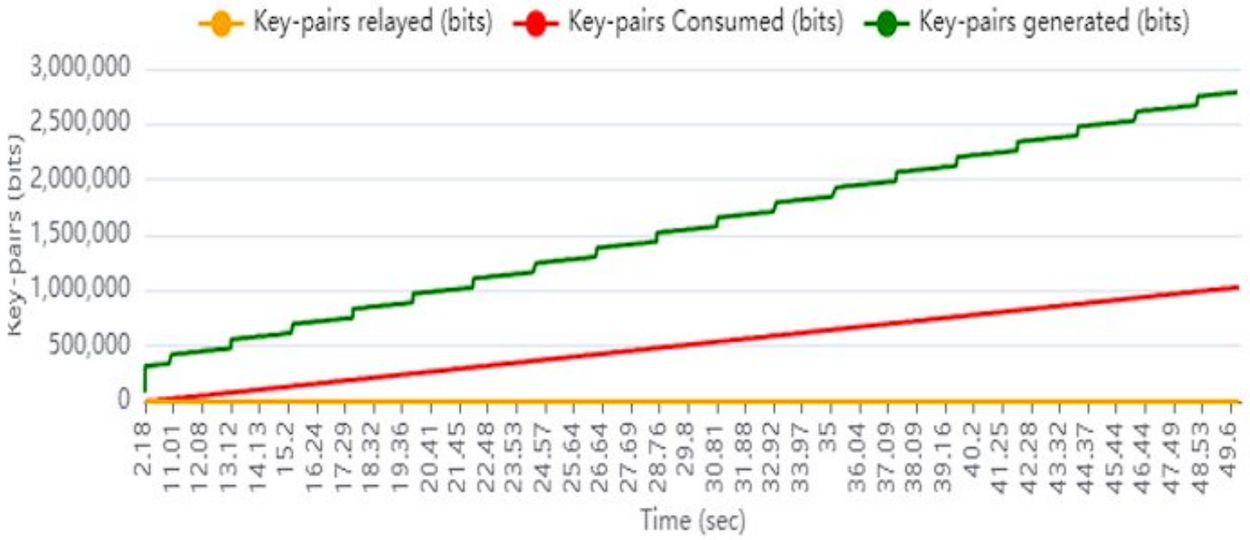
Aplicação	KeyRate	5kbps	10kbps	15kbps	20kbps	100kbps	500kbps
VMAC ou OTP	KDU	23.30%	69.80%	69.80%	77.30%	98.80%	98.80%
	MC	767	302	302	227	2	2
VMAC + OTP	KDU	11.61%	35.10%	47.30%	69.80%	98.80%	98.80%
	MC	884	649	527	302	2	2

Resultados

Dois cenários analisados:

- Rede consumindo mais chaves do que gerado
- Rede gerando mais chaves do que necessário.





Conclusão

Trabalho Preliminar

Simulações para avaliar o comportamento do simulador

Área de pesquisa ativa e inovadora

Projeto de roteamento em redes quânticas

Colaboração

Senai/Cimatec

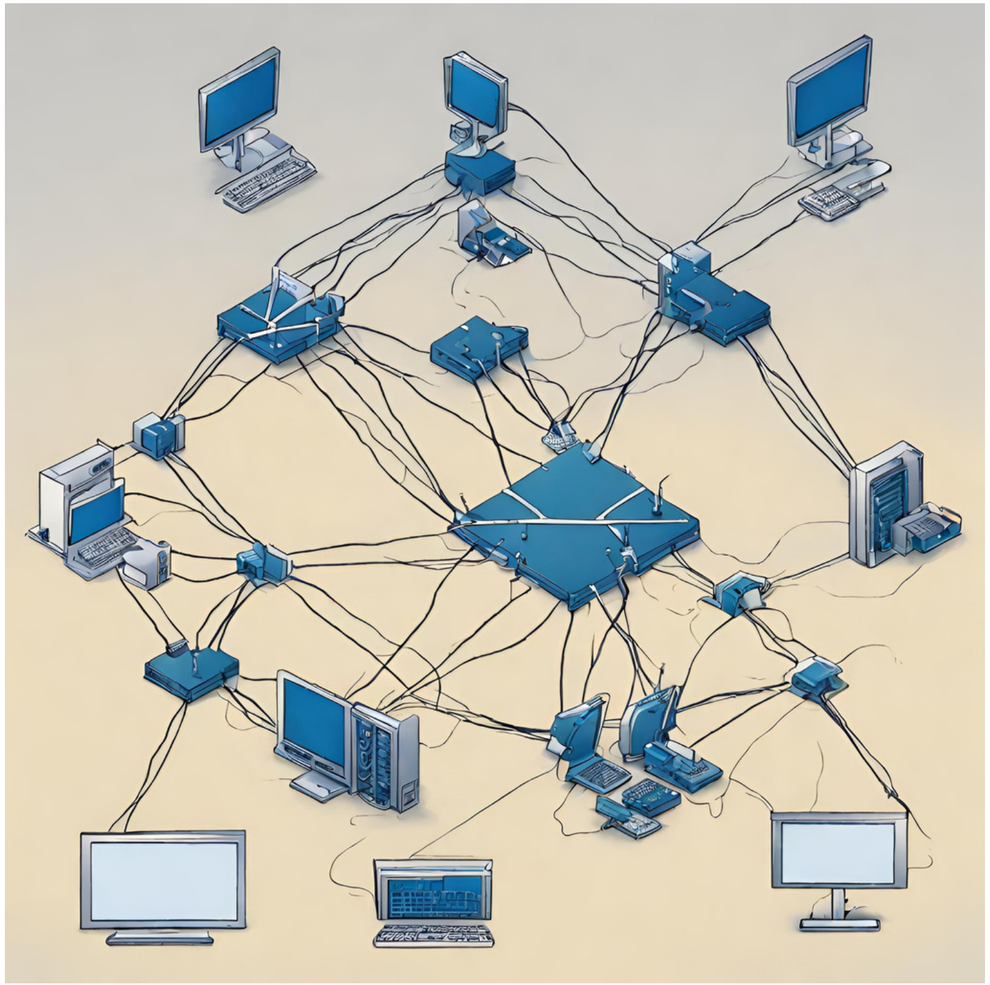
USP

Unicamp

RNP

Trabalhos Futuros

- Otimizar os parâmetros para atender a requisitos de segurança
- Criptografia quântica pode aprimorar a segurança das comunicações
- Importante para futuras iniciativas
- Explorar outras topologia de rede



Obrigado!

Agradecimentos:

GERCOM

UNIVERSIDADE FEDERAL DO PARÁ

FAPESP

CNPq