Alocação de recursos em Redes de Distribuição Quântica de Chaves Multiprotocolo

WPEIF

Autores: Arthur Pimentel, Diego Abreu,
Antônio Abelém

Apresentado por:
Diego Abreu

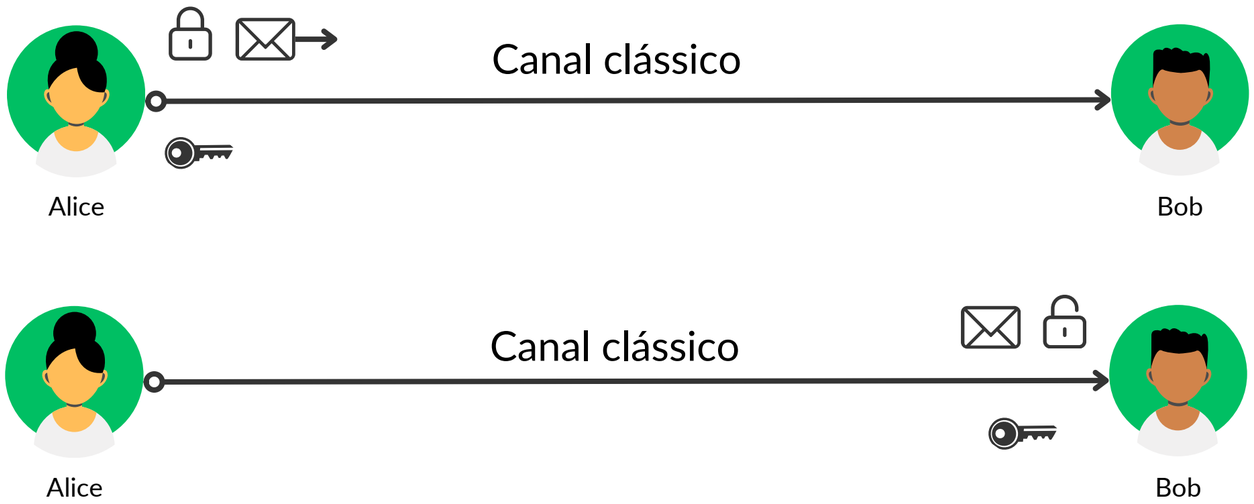
Data:
17 de Maio de 2024

Agenda

GERCOM

- Introdução
- Distribuição Quântica de Chaves
- Proposta
- Estudo de caso
- Resultados

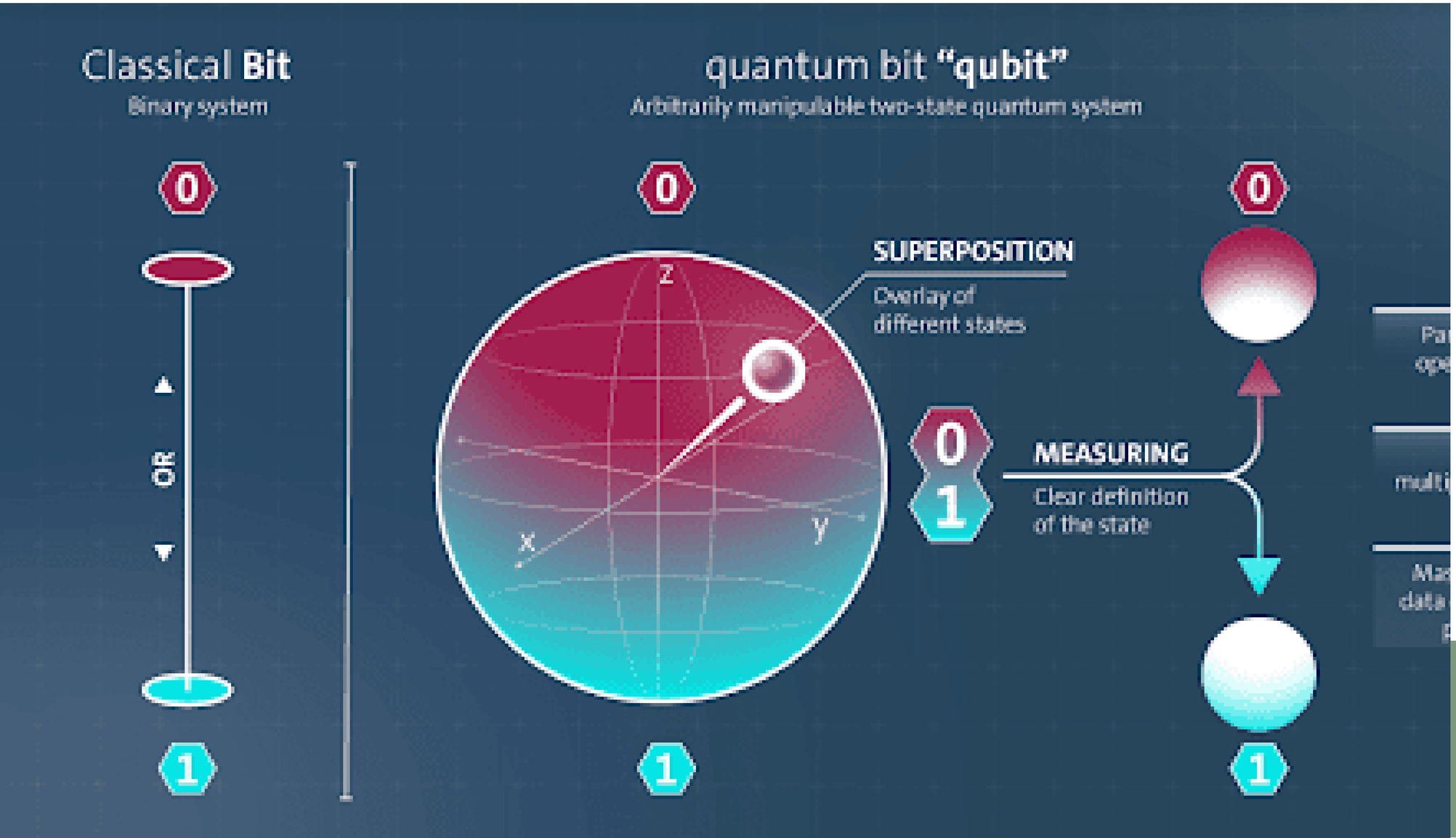
Introdução



- Troca de Chaves Assimétricas
- Computação Quântica
  - Algoritmo de Shor pode quebrar criptografia assimétricas
  - Algoritmo de Groover pode quebrar criptografia simétrica
- Haverst now, decrypt latter
- Criptografia Pós-Quântica é uma alternativa
- Criptografia Quântica Garante a Segurança à nível de rede

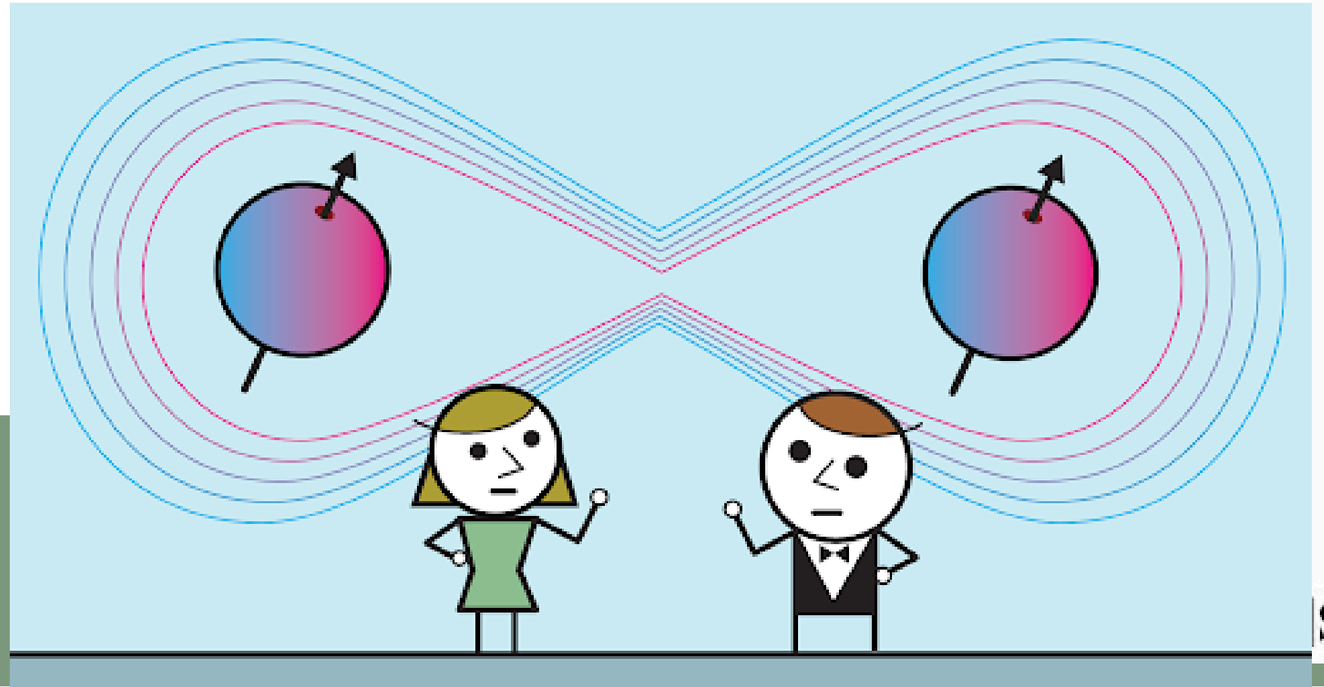
Introdução: Superposição

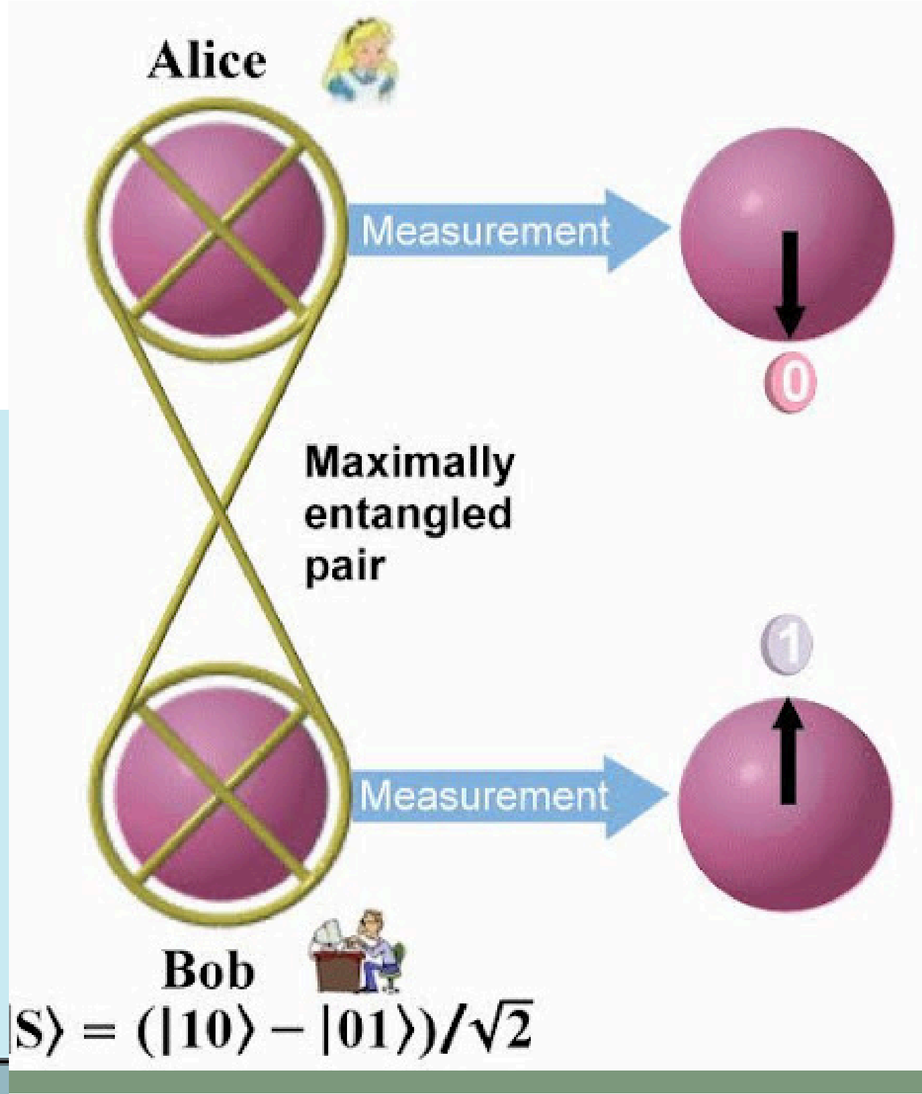
GERCOM



Introdução: Entrelaçamento

- Dois Qubits pode estar entrelaçados
  - Caso um Qubit seja medido, o outro irá colapsar imediatamente
  - Independe da distância
  - Máxima correlação, Máxima Segurança

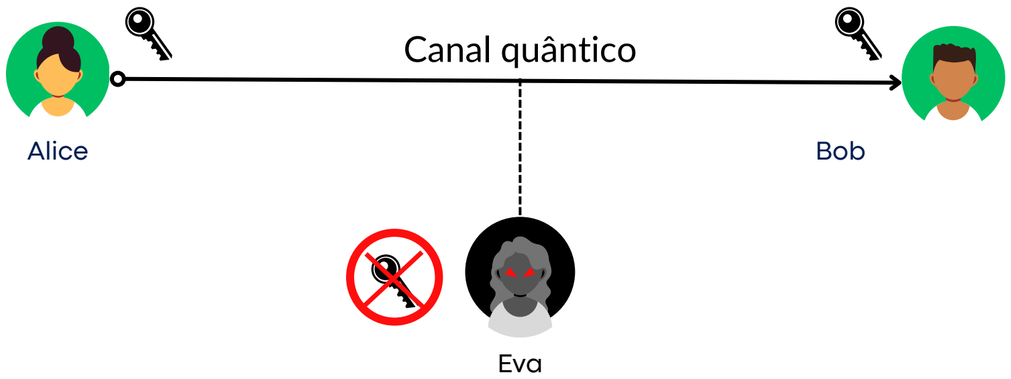




Distribuição Quântica de Chaves

- Compartilhamento seguro de chaves
- Canal Quântico
- Criptografia e autenticação clássica
- Se houver espião, ele será detectada
- A chave não é compartilhada se o canal não for seguro

Funcionamento



Protocolos

- Prepare-and-measure
- Entanglement Based
- BB84, B92, E91

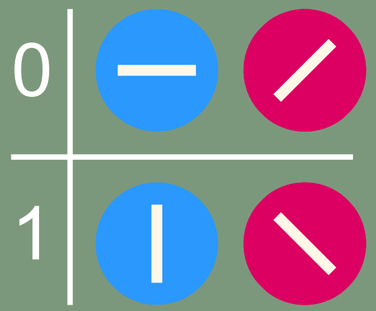
GERCOM

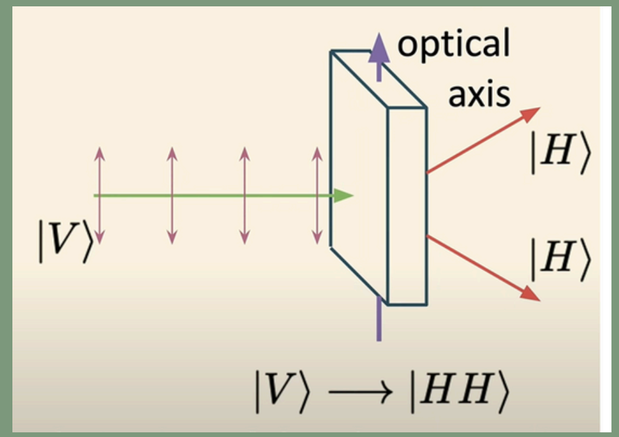
Distribuição Quântica de Chaves

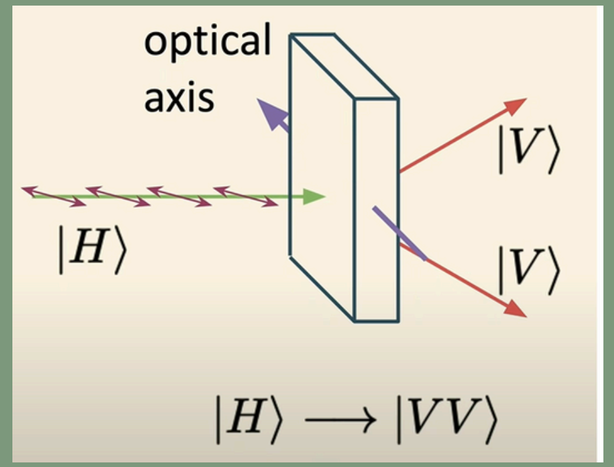
- Há diferentes bases;
- Base nos estados |0⟩ e |1⟩
- ou base nos estados |-⟩ e |+⟩;
- Preparar um qubit em uma base e medir na mesma: Certeza;
- Preparar um qubit em uma base e medir em outra: Aleatoriedade.

Bases:

Estados:



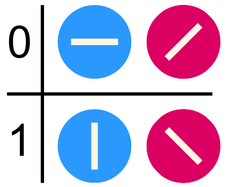




BB84

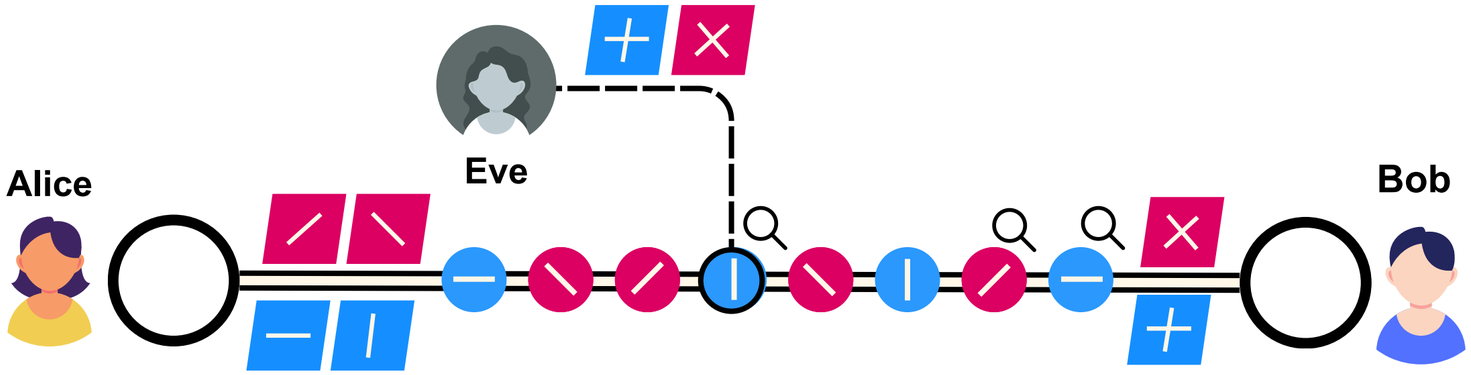
Charles H. Bennett e Gilles Brassard, 1984

Estados quânticos:



- Alice codifica o qubit de acordo com sua chave
- 4 estados
- Comparam as bases

GERCOM



Alice	Bits:	0	1	0	1	1	1	0	1
	Bases:	+	×	×	+	×	+	+	×
	Qubits enviados:	—	\	/	|	\	|	—	\
Eve	Espião:	☐	☐	☐	X	☐	☐	X	X
Bob	Bases:	+	+	×	+	+	×	+	×
	Qubits recebidos:	—	—	/	—	|	/	|	\
	Chave gerada:	0	-	0	0	-	-	1	1

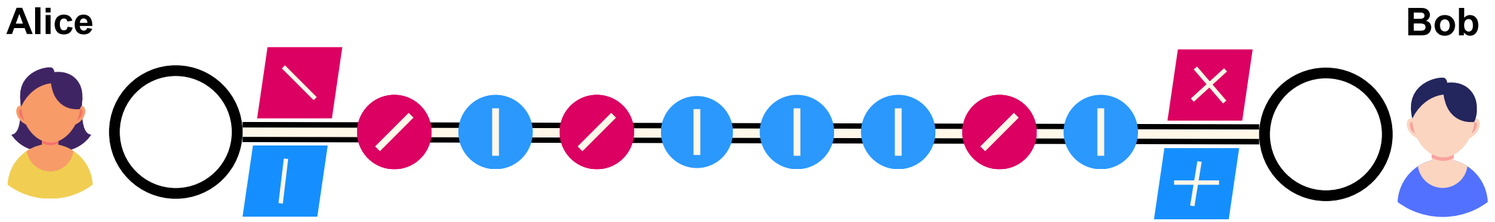
B92

Charles H. Bennett, 1992

Estados quânticos:

0	⟋
1	|

- Deduz-se o bit de Alice
- Dois estados apenas
- Não comparam as bases
- Menos bits



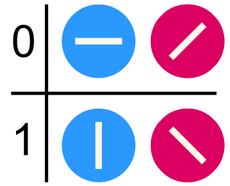
Alice	Bits:	0	1	0	1	1	1	0	1
	Qubits enviados:	⟋	|	⟋	|	|	|	⟋	|
Bob	Bases:	+	+	×	+	+	×	+	×
	Qubits recebidos:	|	|	⟋	|	|	⟋	|	⟍
	Medição:	1	0	0	0	0	0	1	1
	Chave gerada:	0	-	-	-	-	-	1	1

GERCOM

E91

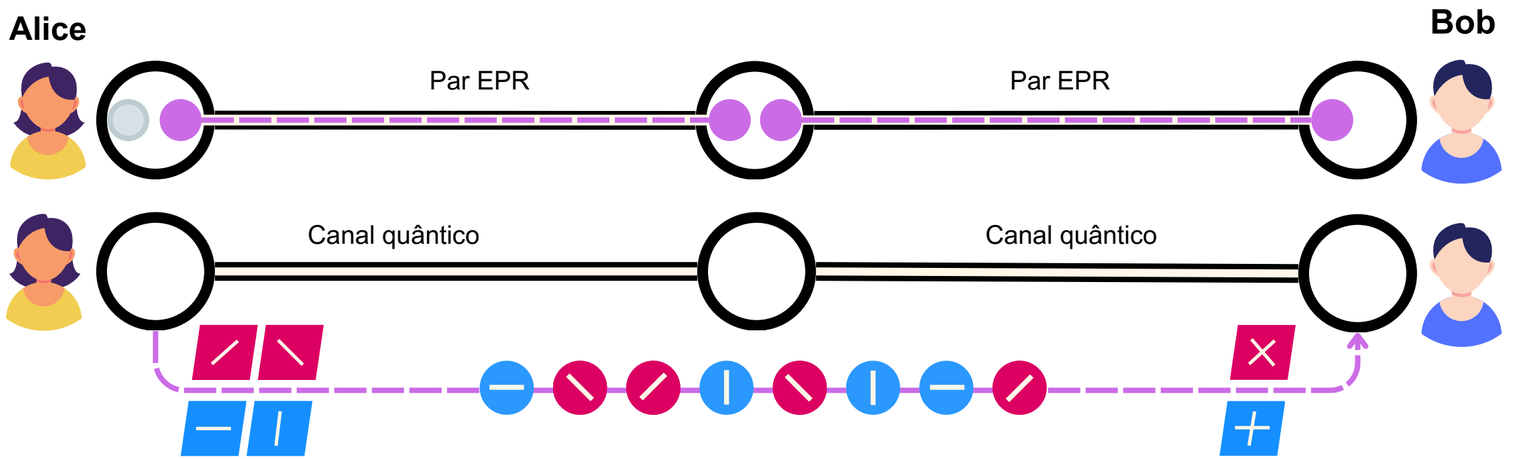
Artur Ekert, 1991

Estados quânticos:



- Mesma lógica BB84
- Não envia o qubit com a mensagem
- Entrelaçamento
- Sem sniffer

GERCOM



Alice	Bits:	0	1	0	1	1	1	0	1
	Bases:	+	×	×	+	×	+	+	×
	Qubits:	—	\	/	|	\	|	—	\
Bob	Bases:	+	+	×	+	+	×	+	×
	Qubits:	—	—	/	|	|	/	—	\
	Chave:	0	-	0	1	-	-	0	1

Alocação de Recursos em Redes QKD Multiprotocolo

GERCOM

Requisições

- Alice e Bob;
- Tipo de protocolo de criptografia;
- Quantidade de chaves necessárias
- Fidelidade miníma requerida
- tempo máximo para atendimento

Tempos da Requisição

- Tempo máximo para o atendimento t1
- Tempo de processamento t2
- Tempo de máximo de início t3

Critérios para alocação

- Em empate, prioriza as requisições com (t1) menor,
- Em seguida, consideramos o (t2)
- Rotas mais curtas tem prioridade
- Taxa de requisições atendidas, eficiência global da rede;

Algoritmo

GERCOM

Algorithm 1 Alocação de Rota e Agendamento de Requisições

Entrada: Lista de requisições R, Rede quântica N, Tentativas máximas k
Saída: Agendamento eficiente das requisições
for cada requisição r em R **do**
    for $i \leftarrow 1$ k **do**
        $rota \leftarrow$ calcularCaminho($r.emissor$, $r.receptor$, N, i)
        if $rota$ não está ocupada na execução atual **then**
            Calcular $t3 \leftarrow r.t1 - TempoAtual$
            Calcular $t2 \leftarrow 1 + \frac{r.tamanhoChaves}{N.qubits \times r.taxaSucessoProtocolo}$
            if $Tempo3 > 0$ **then** ▷ Tempo restante para o prazo final
                Agendar r na $rota$
                break
            end if
        end if
    end for
    if não foi agendada **then**
        Adiar r para próxima execução
    end if
end for

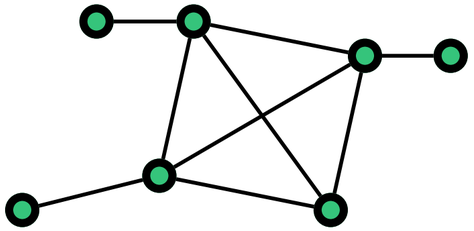
Configuração dos Experimentos

Repositório do artigo:
github.com/artuenric/qkd-net

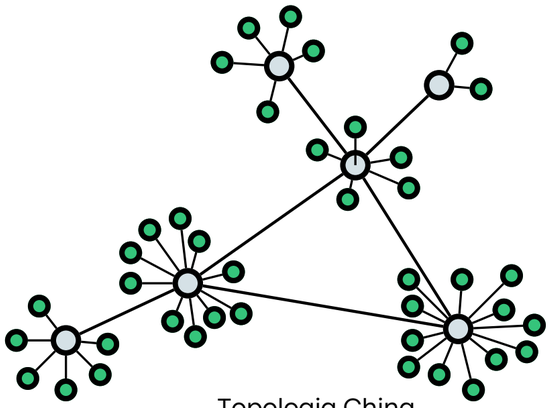
- Estudo de caso com apps de segurança;
- Simulação discreta;
- Linguagem de programação Python.

- App1 requer 100 chaves
- App2 requer 200
- App3 requer 500
- App4 requer 1000
- App5 requer 1500

Aplicação	Caso 1	Caso 2	Caso 3	Caso 4
App1	30%	25%	20%	15%
App2	30%	25%	20%	15%
App3	20%	20%	20%	20%
App4	15%	15%	20%	25%
App5	5%	15%	20%	25%



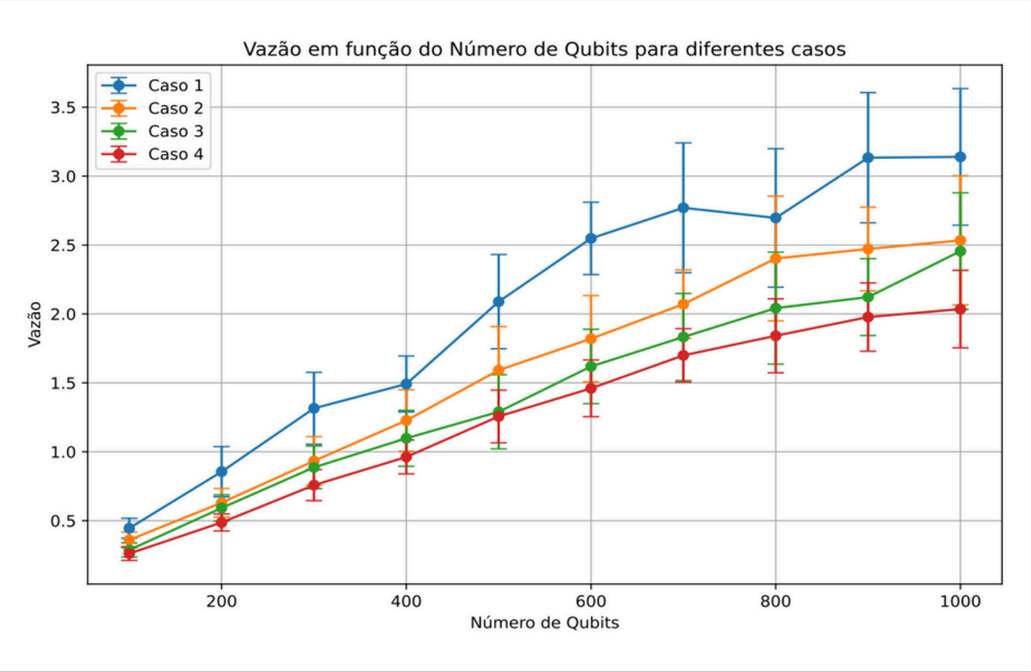
Topologia Viena



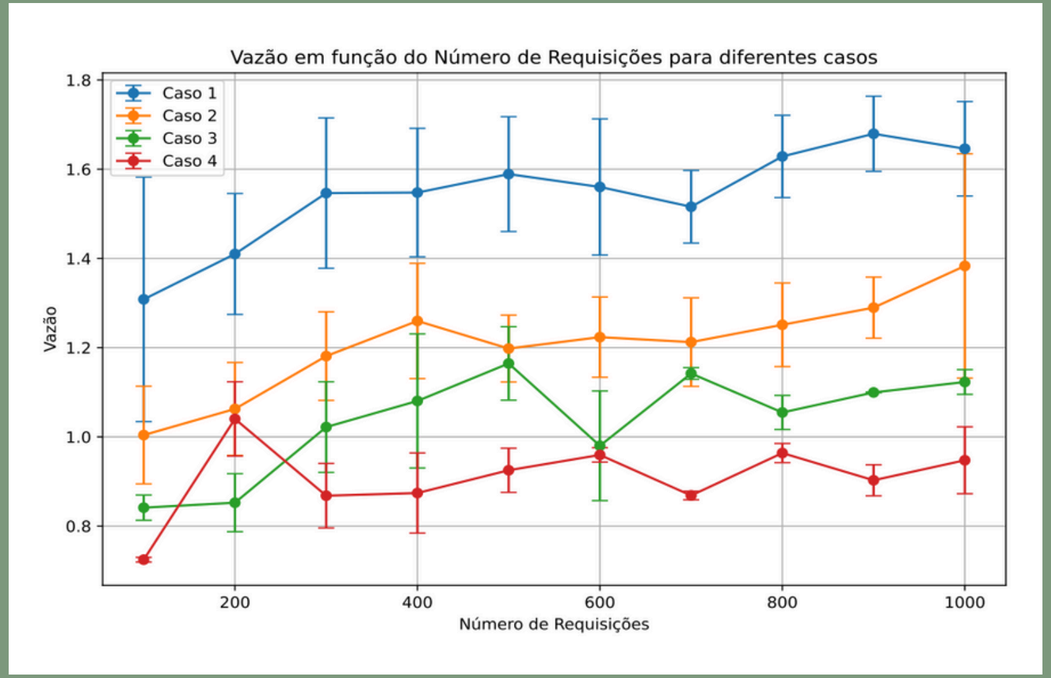
Topologia China

Resultados

Topologia Viena



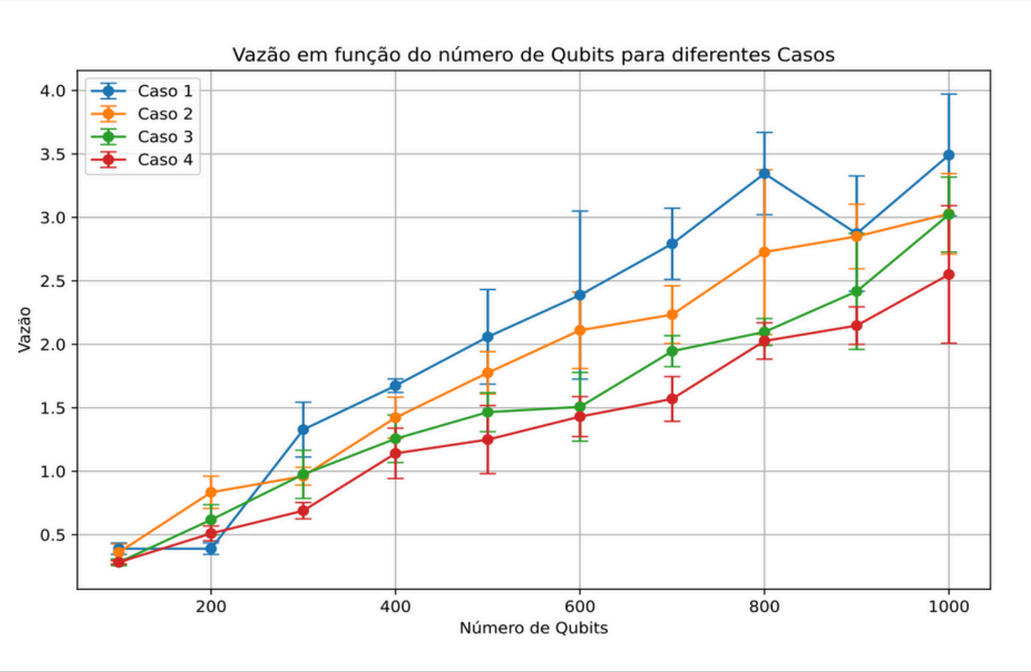
Qubits enviados



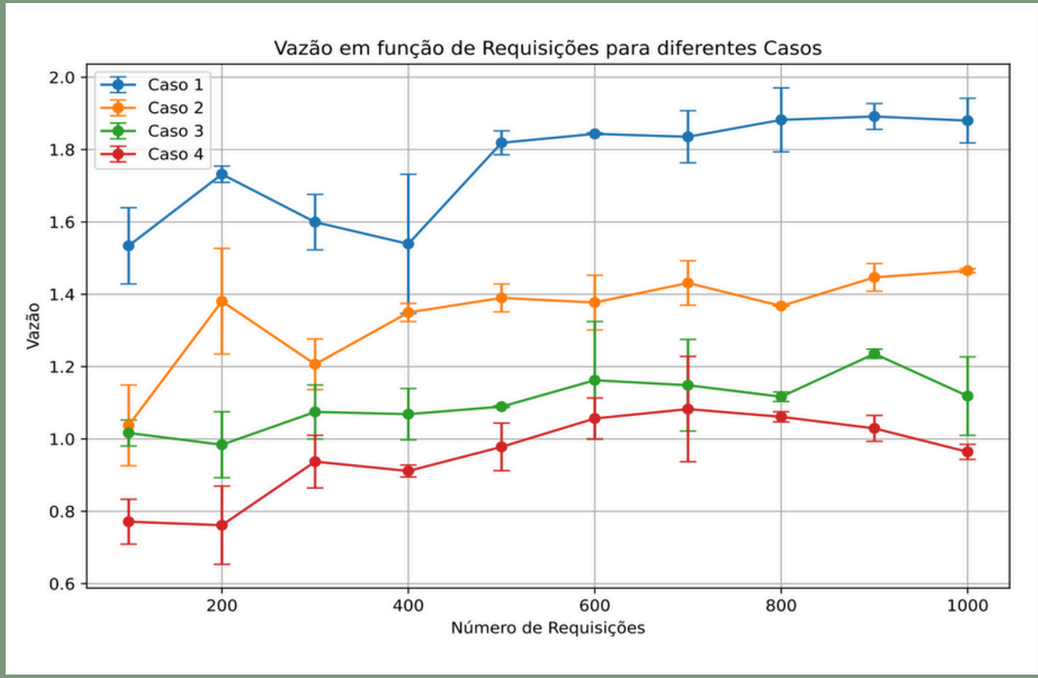
Número de Requisições

Resultados

Topologia China



Qubits enviados



Número de Requisições

Conclusão

- Viabilidade e eficácia da proposta em ambientes de rede multiprotocolo.
- A gestão de recursos e a distribuição adequada das aplicações são essenciais
- Pavimentando o caminho para uma Internet Quântica mais segura e eficiente.

Trabalhos Futuros

- Expansão da arquitetura para variedade maior de cenários de aplicação e desafios
  - tecnologias emergentes de computação quântica
  - novos protocolos QKD
- investigar o impacto da arquitetura em rede de grande escala
- interação com as redes clássicas
- otimização conjunta de recursos
- clássicos e quânticos.

Agradecimentos

Este trabalho foi parcialmente financiado pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) e pela Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), projeto 2020/04031-1, projeto 2021/00199-8 (CPE SMARTNESS), projeto 2023/00673-7 e projeto 2023/00811-0.

OBRIGADO!