Síntese - Advances in the Quantum Internet

Autor
José Lira de Oliveira Junior

2022

Advances in the Quantum Internet - GYONGYOSI

O artigo apresenta o potencial da internet quântica de transformar a comunicação por meio da solução de problemas de segurança.

A internet quântica é baseada nos fundamentos da mecânica quântica e deve fornecer redes de comunicação avançadas e de alta segurança. Além disso, permite aos usuários serviços não disponíveis na internet tradicional.

Tendo em vista que a comunicação tradicional não será mais segura quando computadores quânticos comerciais se tornarem disponíveis, torna-se necessária uma estrutura de rede diferente: a **internet quântica**.

Principais características

- protocolos e fenômenos quânticos avançados;
- segurança incondicional;
- estrutura de rede emaranhada;

Repetidores quânticos

Ao contrário de repetidores tradicionais, repetidores quânticos não podem utilizar o mecanismo de receber-copiar-retransmitir por conta do teorema da não-clonagem.

Memórias quânticas em um repetidor quântico são essenciais para a realização de uma internet quântica. Um desafio relacionado a isso é o ruído quântico que memórias trazem para sistemas quânticos de armazenamento. No entanto, apesar de repetidores quânticos serem possíveis de fabricar sem memórias, estas são necessárias para otimizar qualquer cenário de redes de alta performance.

Iniciativas governamentais

- 2016 - European Quantum Manifesto.
- 2017 - China inicia pesquisa da implementação de uma rede QKD em escala global.
- 2018 - Quantum Technologies Flagship - membros da UE participam da iniciativa EuroQCI (European Quantum Communications Infrastructure).
- 2019 - National Quantum Initiative Act (NQIA) - governo dos EUA estabelece um fundo de pesquisa na área.

O EuroQCI foca em redes de distribuição de chaves quânticas (QKD) ao longo da Europa, as quais podem ser estendidas futuramente para a transmissão de informação quântica entre computadores quânticos.

Redes EuroQCI

Consistem de dois segmentos principais:

- Segmento terrestre (*ground*): conecta sistemas nacionais baseados em fibra óptica por meio de links fronteiriços e contém estações terrestres receptoras de sinais de satélites. Redes de teste tem sido desenvolvidas.
- Segmento espacial (*space*): compartilhará materiais de chaves quânticas secretas entre estações terrestres distantes, seja por meio de satélites LEO (*low earth orbit* ou MEO (*medium earth orbit*) usando protocolos de preparação e medição, ou por meio de satélites geoestacionários (GEO) utilizando protocolos baseados no emaranhamento.

Conceitos preliminares

Uma das principais tarefas de uma configuração quântica de internet é distribuir emaranhamento quântico entre um nó fonte e um nó alvo por meio de nós intermediários chamados **repetidores quânticos**. Isso é alcançado por meio da geração de conexões emaranhadas de curta distância entre nós.

- *Hop distance* (distância do salto): o número de nós entre o nó fonte e o nó alvo de uma dada conexão emaranhada.
- *Entanglement purification and swapping* (purificação e troca de emaranhamento): procedimento aplicado nos nós repetidores para melhorar e estender o emaranhamento.

Tecnologias de implementação de estados quânticos

- **Qubits fotônicos**: utiliza fótons como qubits e dispositivos ópticos. Fótons podem ser controlados e manipulados por dispositivos ópticos padrão. Implementações de baixo custo para fibras ópticas e canais ópticos sem fio, comunicações ópticas, geração e distribuição de emaranhamento, criptografia quântica, e computações ópticas quânticas.
- **Tecnologia de estado sólido**: utiliza spins de elétrons e circuitos supercondutores e interage com dispositivos padrão de RF e microondas. Permite a implementação eficiente por meio de dispositivos semicondutores para desenvolver aplicações de computação em larga escala, memórias quânticas e computadores quânticos.
- **Tecnologia de supercondutores**: utiliza junções Josephson, interconexões, elementos passivos, indutores e capacitores. Permite implementações de alta fidelidade para computação quântica tolerante a falhas, portas quânticas de alta velocidade, computadores quânticos em larga escala e suporta interação com tecnologia de microondas.

- **Eletrodinâmica quântica de cavidade**: utiliza uma interação coerente entre um sistema quântico de matéria e o campo de um ressonador óptico ou de microondas. Permite o acoplamento de átomos com fótons em cavidades para gerar emaranhamento entre átomo-átomo, átomo-fóton e fóton-fóton.

- **Íons aprisionados**: utiliza íons aprisionados para implementar estados quânticos. Permite implementações de alta fidelidade para computação quântica tolerante a falhas, portas lógicas de alta velocidade e aplicações de computação quântica em larga escala com alta conectividade na camada física.

Métodos de geração de emaranhamento

- **Emaranhamento fóton-fóton**: utiliza um feixe de laser e cristal. Fótons são empregados na geração e distribuição de emaranhamento por meio da incidência de um feixe de laser em um cristal. A transmissão de fótons entre pontos distantes pode ser implementada por meio de fibra óptica com baixa atenuação. **Alta taxa de sucesso.**

- **Emaranhamento fóton-átomo**: utiliza uma cavidade óptica e um feixe de laser. Átomos são acoplados com uma cavidade óptica. Na fase de emeissão, um feixe de laser resulta em fótons-átomos emaranhados na cavidade do emissor. Na fase de absorção, fótons são absorvidos e mapeados no estado de átomos remotos na cavidade do receptor. Átomos emissores e receptores são emaranhados por fótons, e o canal de comunicação pode ser implementado por um canal óptico. **Baixa taxa de sucesso.**

- **Emaranhamento átomo-átomo**: utiliza um feixe de laser, cavidade óptica e medição no canal quântico entre emissor-receptor. Nas cavidades do emissor e receptor, dois átomos são simultaneamente excitados por um feixe de laser, resultando em dois fótons emaranhados por átomo (?). Então, são transmitidos da cavidade do emissor e receptor por meio de um canal óptico, no qual os fótons são medidos. **Baixa taxa de sucesso.**

Estratégias de distribuição de emaranhamento

Tabela 1: Estratégias de distribuição de emaranhamento

Estratégia	**Dinâmica de interação**	**Implementação**
Interação direta	A e B interagem diretamente pelo hamiltoniano H_{AB}	Interação direta entre A e B e transmissão direta do subsistema emaranhado A ou B
Interação indireta	A e B não interagem diretamente. Não há H_{AB}	Interação indireta entre A e B, transmissão do sistema auxiliar C
Interação discreta	A e B não interagem diretamente. Não há H_{AB}	Alice emaranha A e C, Bob realiza o swap em B e C para emaranhar A e B.
Interação contínua	A e B não interagem diretamente. Não há H_{AB}	O sistema auxiliar C media interações contínuas entre A e B para emaranhar A e B.

A tabela 1 resume as características de diferentes estratégias de distribuição de emaranhamento, as quais são ilustradas na Fig. 1, na qual $\mathcal{N}$ representa um canal quântica que pode ser implementado por fibra óptica ou um canal óptico sem fio.

A transmissão direta de um estado emaranhado (correlação quântica) necessita de um canal com alta fidelidade, enquanto que a transmissão direta de um estado separável (correlação clássica) pode ser implementada por meio de um canal quântico mais ruidoso.

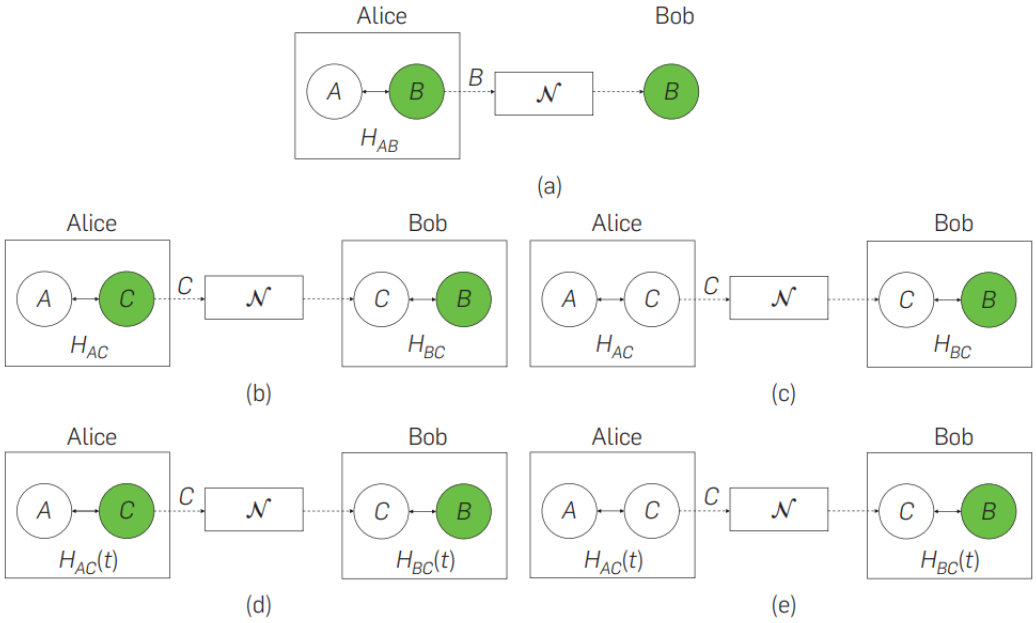

Figura 1: interações: a) direta, b) indireta e discreta com *flag* emaranhada C, c) indireta, discreta com *flag* separável C, d) indireta, contínua com *flag* emaranhada C, e) indireta, contínua com *flag* separável C

Estruturas emaranhadas e não emaranhadas da internet quântica

Redes quânticas de comunicação podem ser classificadas em:

- emaranhadas;
- não emaranhadas.

Nas redes não emaranhadas, as conexões entre nós quânticos são formadas por meio de estados quânticos não emaranhados. Em uma rede emaranhada, conexões entre nós quânticos são realizadas por estados emaranhados. Estes estados emaranhados são armazenados em memórias internas nos nós quânticos. As características e objetivos dos dois tipos de rede são fundamentalmente distintos.

O objetivo principal de uma rede **não emaranhada** é implementar um protocolo QKD (ou geração de números aleatórios) padrão ponta-a-ponta entre nós. Já em uma rede **emaranhada**, o propósito principal é distribuir emaranhamento quântico a longas distâncias.

Os serviços dos dois tipos de rede podem ser utilizados para melhorar redes tradicionais, garantindo criptografia mais poderosa e serviços de segurança, como o IPSec (*Internet Protocol Security* ou TLS (*Transport Layer Security* com QKD.

Em um cenário de internet quântica, a rede fundamental é uma rede quântica emaranhada e o objetivo principal é fornecer uma estrutura de rede geral para computadores quânticos de forma que estes possam estabelecer comunicação segura e eficaz a longas distâncias. Assim, **emaranhamento e repetidores** são elementos essenciais na construção da internet quântica.

Uma conexão emaranhada é criada por EDP (*entanglement distribution process*) por meio de vários links físicos. A distribuição de emaranhamento é, por vezes, referida como o processo de distribuir o emaranhamento por ligações curtas. Alguns protocolos importantes para alcançar isso são *meet-in-the-middle* (encontrar-se no meio) ou *sender-receiver* (emissor-receptor).

É válido ressaltar que QKD não garante comunicação quântica segura, mas pode ser usada para gerar uma chave clássica segura entre duas partes. Além disso, QKD também não fornece criptrografia forte, já que simplesmente gera uma chave clássica segura, a qual pode ser utilizada em métodos como AES (*Advanced Encryption Standart*) ou criptografia OTP (*one-time pad*), a qual seria perfeitamente segura dada uma chave completamente aleatória.

Em uma rede quântica, há duas formas principais de conectar dispositivos quânticos:

- **emaranhamento bipartido** - na forma de pares de Bell. Pares de Bell são suficientes para gerar qualquer estado arbitrário, seja mesclando-os ou preparando o estado localmente e realizando o teleporte pela rede, o que é bastante custoso em termos de recursos.

- **emaranhamento multipartido** - os dispositivos são conectados usando emaranhamento multiparte ou estados aglomerados (*cluster*). Esse tipo de rede oferece uma vantagem em relação ao uso de pares de Bell: ao compartilhar estados grafos (?) ou outros estados multiparte, os dispositivos da rede (ou clientes) precisam aplicar menos operações no final, o que é uma vantagem significativa supondo canais ruidosos.

Pode-se concluir que, por mais que sejam mais difíceis de implementar, redes quânticas que utilizam estados multipartidos introduzem menos ruído nos sistemas quânticos em um cenário realístico.

Distribuição de emaranhamento por arquitetura de duplicação

A meta é gerar emaranhamento de longas distâncias entre dois nós A e B por meio de uma cadeia de repetidores. A arquitetura define diferentes níveis de emaranhamento, 1, 2, 3, 4. Cada incremento de nível dobra a distância do salto.

- $l = 1$ - nível 1: conexões são estabelecidas entre todos os nós e o swap é aplicado nos repetidores.

- $l = 2$ - nível 2: conexões são geradas pelos repetidores R_1, R_3, R_5 e R_7.
- $l = 3$ - nível 3: conexões são geradas pelos repetidores R_2 e R_6.
- $l = 4$ - nível 4: a conexão entre A e B é gerada por R_4.

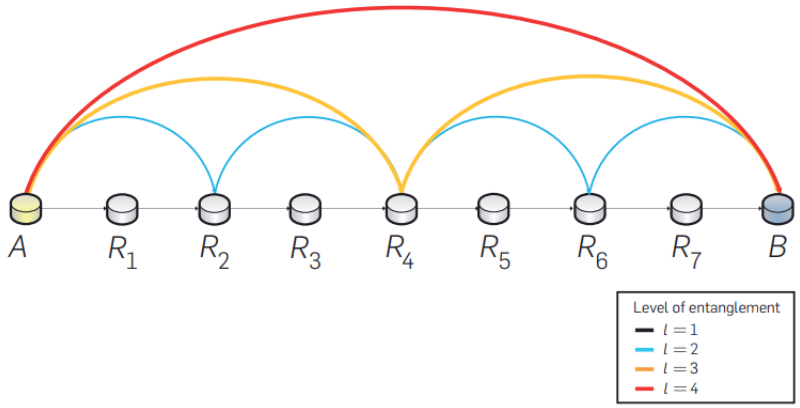

Figura 2: Distribuição de emaranhamento por arquitetura de duplicação

Arquitetura geral da internet quântica

A Fig. 3 mostra a arquitetura geral da internet quântica. O modelo consiste de um conjunto de usuários com dispositivos quânticos e clássicos, repetidores intermediários com um conjunto de conexões emaranhadas com diferentes níveis de emaranhamento.

Além disso, a internet quântica integra fibra óptica e canais ópticos sem fio entre repetidores *ground-to-ground* e canais ópticos espaciais *ground-to-satellite*.

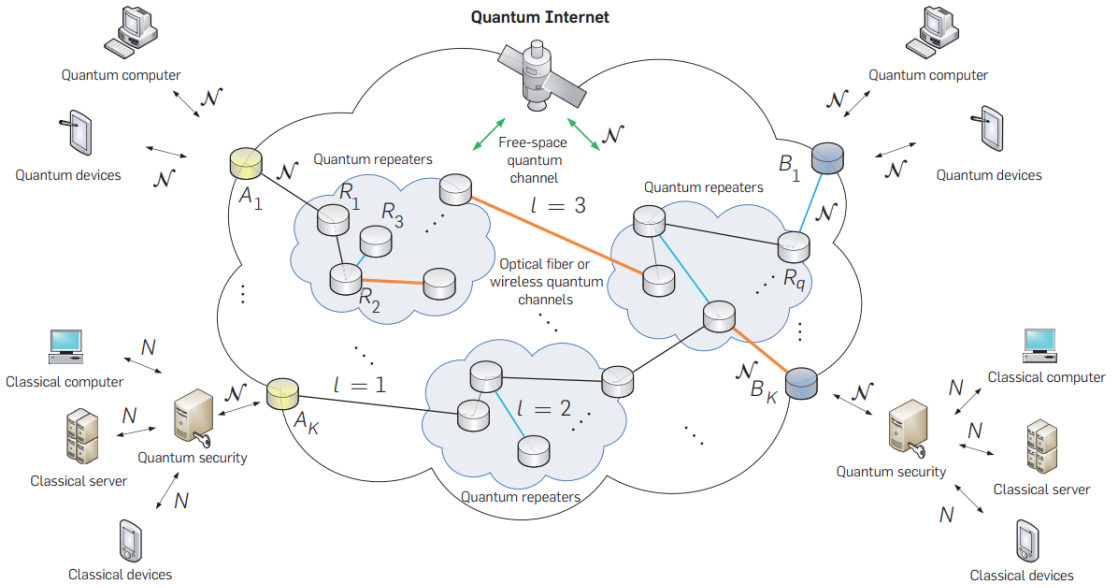

Figura 3: Arquitetura geral da internet quântica

Interoperabilidade da internet quântica e clássica

A curto prazo, a internet quântica irá funcionar em paralelo com a internet clássica. Os dispositivos quânticos se comunicam por meio de um canal quântico $\mathcal{N}$ com a noção abstrata de nuvem da internet quântica, enquanto que dispositivos clássicos utilizam um protocolo quântico, como o QKD, para acessar a internet quântica, além de poderem acessar a internet clássica normalmente.

O canal de comunicação entre dispositivos clássicos e o protocolo quântico é um canal clássico N.

Propostas

Operações e transmissão de informação avançadas

Enquanto que um canal de comunicação clássico permite o envio de informação clássica apenas, um canal quântico estende as possibilidades. Pode transmitir informação clássica, funcionando como um link clássico; pode transmitir informação clássica privada (QKD); pode transmitir informação quântica (superposição ou emaranhamento).

Protocolo de pilha do repetidor quântico

Este protocolo descreve as interações de distribuição de emaranhamento entre nós quânticos.

A camada mais baixa da pilha é a **camada física**, a qual descreve apenas as comunicações quânticas puras, como a transmissão direta de emaranhamento por canais físicos entre nós vizinhos.

A próxima camada, a **camada de controle de emaranhamento**, define métodos de controle para as transmissões pela camada física; essas duas camadas são definidas entre todos os nós quânticos diretamente conectados. A comunicação é unidirecional apenas nessas duas camadas, nas camadas superiores, é bidirecional. O processo de transmissão de emaranhamento na camada física começa em Alice em direção a Bob pelos nós intermediários diretamente conectados (conexões de nível 0).

As duas próximas camadas - **controle de purificação de emaranhamento** e **controle de troca de emaranhamento** - são definidas somente entre nós quânticos envolvidos nestes processos na arquitetura de duplicação.

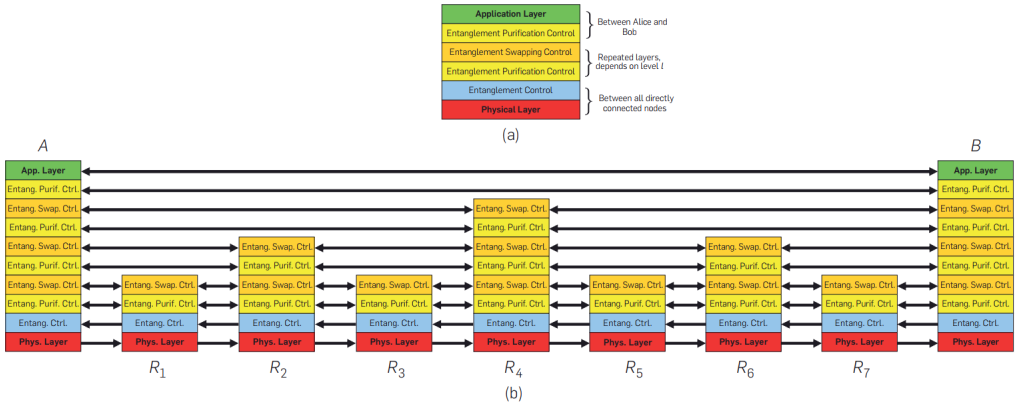

Figura 4: Protocolo de pilha nos repetidores

O protocolo descrito é mostrado na Fig. 4. Em Fig. 4.a, tem-se a estrutura geral, já em Fig. 4.b, tem-se as interações do protocolo para uma arquitetura de duplicação de nível $l = 4$.

Segurança avançada

Redes clássicas não permitem segurança incondicinoal para as partes com complexidade computacional razoável. No entanto, na internet quântica, isto é um serviço padrão. A segurança avançada é fornecida pelo protocolo QKD e funções de criptografia distribuídas (acordo bizantino, eleição de líder, computação quântica cega, etc).

Os primeiros protocolos QKD introduzidos foram baseados em variáveis discretas (DV), como polarização de fótons. O primeiro protocolo DVQKD foi o chamado BB84, que utiliza polarização de fótons únicos para codificação.

Tendo em vista que a polarização de fótons únicos não pode ser codificada e decodificada eficientemente por conta de limitações tecnológicas dos dispositivos atuais, sistemas QKD com variáveis contínuas foram propostos. Em um CVQKD, a informação é codificada em variáveis contínuas (isto é, pacotes de fótons (?)) por meio de uma

modulação Gaussiana usando a quadratura da posição ou do momento de estados quânticos coerentes. Esse método pode ser realizado por dispositivos padrão, atualmente disponíveis e amplamente utilizados em redes de telecomunicações.

Possibilidades avançadas na engenharia

A principal tarefa da camada física na internet quântica é a transmissão confiável de estados quânticos e o armazenamento interno fiel de estados quânticos recebidos em memórias quânticas nos nós.

Isto requer colaboração entre a rede e serviços de gerenciamento em um nível lógico mais alto. A camada lógica utiliza a informação clássica de uma rede quântica por meio de canais tradicionais para fornecer um *feedback* e um mecanismo de adaptação para a camada física.

A camada lógica contém tafeas de controle e pós-processamento, como correção de erros, monitoramento dinâmico de ligações e memórias quânticas, controle de armazenamento interno e mecanismos de correção de erro em nós, otimização de rede e processos avançados de gerenciamento de serviços.

Os **principais desafios** na área da internet quântica são:

- soluções para transmissão de sistemas emaranhados;
- otimização da arquitetura de rede;
- desenvolvimento de serviços de rede para distribuição de emaranhamento.

Computação distribuída avançada

Computação baseada em medição está no coração da computação quântica distribuída usando emaranhamento como um recurso. O objetivo de medições quânticas é extrair informações úteis e valiosas de um estado quântico medido. Enquanto que a entrada de uma medição pode ser um estado quântico superposto ou emaranhado, a saída é informação clássica, isto é, *strings* de bits.

Roteamento de emaranhamento quântico

Em uma rede quântica emaranhada, encontrar o caminho mais curto entre nós quânticos arbitrários é crucial para transmitir uma mensagem entre nós no menor número de etapas possíveis. Tendo em vista que não há conhecimento global, em cenários práticos, sobre os nós ou propriedades das conexões emaranhadas, o roteamento deve ser feito de modo descentralizado. Um roteamento descentralizado só pode utilizar o conhecimento local sobre os nós, seus vizinhos e seu nível compartilhado de emaranhamento.

Além disso, também foi proposto o modelo oportunista de distribuição de emaranhamento. Este método fornece distribuição eficiente de emaranhamento, fácil aplicação e solução moderadamente complexa para distribuição de emaranhamento com alta fidelidade em cenários experimentais de internet quântica.

Bases de implementação

Uma implementação prática de internet quântica integra:

- dispositivos fotônicos;
- memórias quânticas;
- cavidades ópticas;
- dispositivos fundamentalmente físicos necessários para a comunicação de redes;
- links padrão (fibra óptica, canais sem fio, comunicação via satélite);
- protocolos fundamentais de redes quânticas.

Experimentos

A internet quântica experimental está em fase de desenvolvimento e existe em laboratórios de física, além de abordagens teóricas. Ainda é necessário encontrar soluções para problemas de engenharia na implementação de dispositivos necessários.

Uma abordagem promissora destes problemas é a formação do grupo QIRG (*Quantum Internet Research Group*), que já possui suporte internacional e colaboração de pesquisas. O QIRG definiu um roteiro técnico com metas para o desenvolvimento da internet quântica experimental.

Links

- Editar no Overleaf: `https://www.overleaf.com/4368184346jdhhxfvsshgv`
- Visualizar no Overleaf: `https://www.overleaf.com/read/kmtymhmpmxwf`