Alocação de Recursos em Redes de Distribuição Quântica de Chaves Multiprotocolo

Arthur Pimentel [1], **Diego Abreu**[1], **Antônio Abelém**[1]

[1]Instituto de Ciências Exatas - Universidade Federal do Pará - UFPA, Belém, Pará

Abstract. *As quantum cryptography advances, it becomes crucial to develop methods that optimize resource usage in Quantum Key Distribution (QKD) networks. Facing the challenge of efficiently scheduling and allocating requests this study proposes an approach for multiprotocol QKD networks using quantum resource-aware routing and scheduling strategies. Our model focuses on improving efficiency in the use of quantum keys, routes, and requests, while supporting various quantum communication protocols. Using two real-world QKD topology networks, we tested our proposal in two application scenarios, with different distributions of authentication and cryptography application requests, evaluating the impact of qubit capacity, and request load. The results demonstrate the feasibility of our approach in diverse operational environments.*

Resumo. *À medida que a criptografia quântica avança, torna-se cada vez mais importante desenvolver métodos que aprimorem a utilização de recursos em redes de Distribuição Quântica de Chaves (QKD). Enfrentando o desafio de agendar e alocar eficientemente as requisições em redes QKD, este estudo propõe uma abordagem para redes QKD multiprotocolo usando estratégias de roteamento e agendamento conscientes de recursos. Nossa proposta foca em melhorar a eficiência no uso de chaves quânticas, rotas e requisições, enquanto suporta vários protocolos de comunicação quântica. Utilizando duas topologias de redes QKD reais, a proposta foi avaliada em dois cenários de aplicação, com diferentes distribuições de requisições de aplicações de autenticação e criptografia. Avaliou-se o impacto da capacidade de qubit e quantidade de requisições. Os resultados demonstram a viabilidade de nossa abordagem em diversos ambientes.*

1. Introdução

A crescente necessidade de distribuição segura de chaves criptográficas em uma variedade de aplicações tem se tornado um aspecto crucial na era da informação digital [Ribezzo et al. 2023]. Nesse cenário, a Distribuição Quântica de Chaves (*Quantum Key Distribution* - QKD) [Cao et al. 2022a] tem sido proposta como uma alternativa segura ao atual esquema de distribuição de chaves públicas, ao utilizar princípios da comunicação quântica para garantir uma troca de chaves robusta e resistente a possíveis ataques. Nesse contexto, redes de distribuição quântica de chaves têm sido propostas para fornecer serviços de QKD em larga escala [Tavares et al. 2023]. Exemplos notáveis incluem as redes QKD na China [Xu et al. 2020] e na Europa [Ribezzo et al. 2023], que já oferecem uma variedade de serviços e implementações de diferentes de protocolos QKD. Esses avanços apontam para o desenvolvimento de uma Internet Quântica, na qual a rede quântica irá

prover diversas aplicações como criptografia, autenticação e computação quântica distribuída [Abelém et al. 2020].

No entanto, à medida que as redes QKD se tornam mais complexas e diversificadas, garantir seu funcionamento e qualidade de serviço torna-se um desafio significativo. Redes QKD multiprotocolos, que incorporam uma variedade de tecnologias e protocolos QKD, oferecem serviços QKD com diferentes níveis de segurança e tecnologia de implementação. A gestão e o controle eficazes dessas redes são essenciais para garantir a integridade e a disponibilidade da comunicação quântica, sem que isso interfira no funcionamento da Internet clássica, principalmente em tarefas como roteamento e agendamento de requisições [Abreu et al. 2022]. O objetivo deste trabalho é propor uma estratégia de alocação eficientemente das requisições em redes QKD que atenda às demandas crescentes das redes QKD Multiprotocolo. Essa abordagem busca aperfeiçoar a utilização dos recursos disponíveis e melhorar a qualidade de serviço na distribuição quântica de chaves.

Enquanto alguns trabalhos, como o de Cao et al. (2018)[Cao et al. 2018], se concentram na alocação de chaves em redes QKD com WDM, utilizando algoritmos de roteamento e alocação específicos, nossa proposta se diferencia ao incorporar a flexibilidade de um sistema multiprotocolo QKD, oferecendo uma abordagem mais abrangente. Outros estudos, como os de Fu et al. (2020) [Fu et al. 2020] , Yu et al. (2023) [Yu et al. 2023] e Zhang et al. (2023) [Zhang et al. 2023], abordam aspectos como otimização da taxa de chaves seguras, eficiência energética e roteamento de recursos, mas nenhum deles considera uma rede multiprotocolo. Por outro lado, os trabalhos de Cao et al. (2022c) [Cao et al. 2022c] e Cao et al. (2022b) [Cao et al. 2022b] exploram redes quânticas multiprotocolo, destacando a importância da flexibilidade e adaptabilidade na infraestrutura de redes quânticas. Nossa proposta se destaca ao integrar ambas as abordagens, combinando o sistema multiprotocolo com o gerenciando eficazmente recursos como requisições, rotas e chaves, configurando uma solução completa para aplicações de autenticação e criptografia. Nossas contribuições consistem na Implementação em ambiente simulado de protocolos QKD e da estratégia de alocação de recursos na arquitetura proposta, e Análise do funcionamento da proposta em duas topologias de redes QKD reais, em cenários de aplicação de segurança, variando a distribuição das requisições e avaliando o impacto das métricas da rede.

2. Distribuição Quântica de Chaves

A Distribuição Quântica de Chaves busca compartilhamento seguro de chaves públicas, as quais podem ser utilizadas em aplicações de segurança, como criptografia de dados e autenticação. Os protocolos de QKD utilizam propriedades da física quântica, como a superposição e o entrelaçamento quântico [Abelém et al. 2020].

O protocolo BB84 [Bennett and Brassard 2014], realiza o processo de QKD utilizando duas bases de medição, retilínea (+) e diagonal (X), com dois estados quânticos (0 e 1) em cada base. O funcionamento do protocolo é ilustrado na Figura 1. No BB84, o objetivo é enviar chaves utilizando qubits (bits quânticos) do ponto A (*Alice*) ao ponto B (*Bob*). Inicialmente, *Alice* prepara o qubits conforme os bits clássicos da chave que deseja compartilhar, e define uma base de medição. Nesse caso, cada qubit codifica um bit da chave a ser compartilhada. Os qubits são então enviados através do canal quântico

até *Bob*. *Bob* recebe os qubits e escolhe as bases para medi-los. Se as bases escolhidas por *Alice* e *Bob* para um qubit forem a mesma, o resultado da medição deve corresponder ao valor enviado por *Alice* e será adicionado à chave compartilhada, se as bases forem diferentes então ela deve ser descartada. A qualidade do qubit transmitido depende da qualidade do canal quântico, e é medida através da fidelidade do canal. A fidelidade pode ser calculada pela fórmula: Fidelidade = $\langle\psi|\rho|\psi\rangle$, onde $|\psi\rangle$ é o estado quântico ideal e ρ é o estado quântico real recebido.

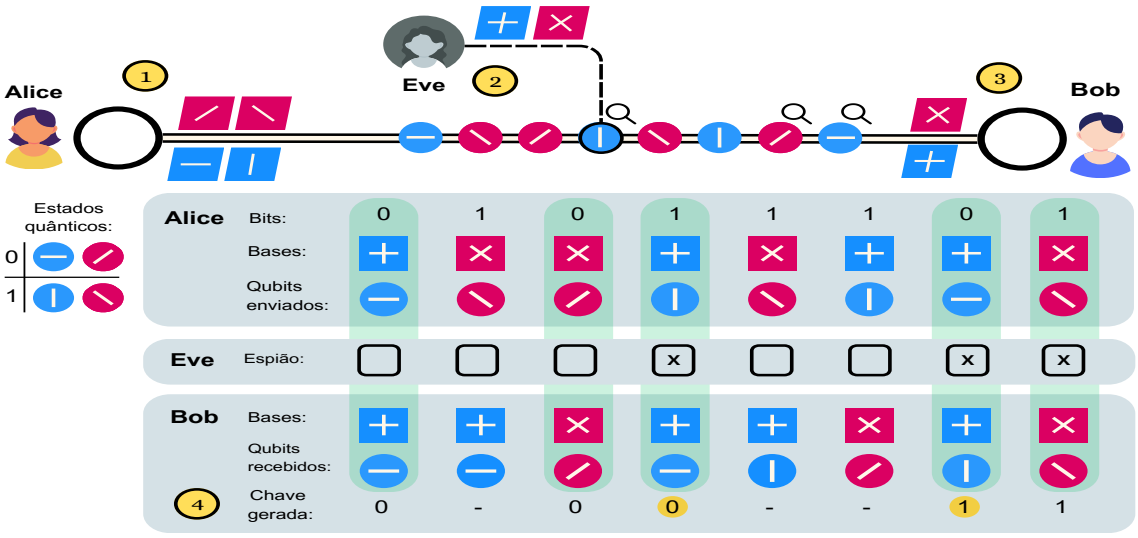


Figura 1. Funcionamento do Protocolo BB84.

Na comunicação entre *Alice* e *Bob*, se um agente malicioso (*Eve* - *eavesdropper*) tentar interceptar os qubits, isso será detectado, em função da propriedade da não-clonagem quântica [Abelém et al. 2020]. Quando *Eve* tenta medir os qubits enviados por *Alice* para *Bob*, ela também precisa escolher uma base de medição. Mesmo que ela escolha a base correta, o qubit será alterado para um estado específico (zero ou um) devido à medição. No caso de Eve gerar novos qubits para *Bob*, na tentativa de evitar ser detectada, quando as bases de medição de *Bob* e *Alice* forem comparadas, eles obterão chaves finais diferentes, mesmo que Eve tenha usado a mesma base que *Alice*.

O protocolo B92 [Bennett 1992], funciona de modo semelhante ao BB84, utilizando duas bases de medição, porém é usado somente um estado de cada base para realizar o compartilhamento da chave. No protocolo B92, inicialmente é associado um estado de base para cada valor dos bits clássicos. *Alice* então envia os qubits em uma única base para todos os bits de valor 0 na chave e faz o mesmo para os bits de valor 1. Os qubits são inicializados como 0, e somente a base é modificada para corresponder aos bits clássicos da chave. *Bob*, por sua vez, escolhe aleatoriamente as bases para medir os qubits que recebe. Os valores que serão adicionados à chave compartilhada não são determinados pelo resultado da medição em si, mas são inferidos com base na combinação da base utilizada por *Bob* e o resultado da medição. Se a base de *Bob* for igual à de *Alice* ao medir um qubit, o resultado será sempre 0, pois o qubit foi inicializado como 0. No entanto, se as bases forem diferentes, o qubit pode colapsar em 0 ou 1, devido à superposição. Quando o qubit colapsa em 0, a base escolhida por *Alice* permanece desconhecida, e *Bob* deve descartar essa medição. Por outro lado, se o resultado for 1, isso indica que as

bases de *Alice* e *Bob* eram diferentes, e *Bob* pode adicionar o valor correspondente à base de *Alice* à chave compartilhada. Portanto, ao final do processo, *Bob* obtém uma chave sem a necessidade de comparar as bases. Ele informa quais qubits adicionou à chave e, em seguida, compara uma parte dela com *Alice* para verificar a integridade e segurança da rede, assegurando a ausência de agente interceptador (*Eve*).

De outro modo, o protocolo E91 [Ekert 1991], se baseia na utilização de pares entrelaçados de partículas quânticas, conhecidos como pares de Einstein-Podolsky-Rosen (EPR). Assim como o protocolo BB84, o E91 também faz uso de duas bases com dois estados cada para codificar e transmitir informações. No protocolo E91, *Alice* e *Bob* compartilham pares EPR de partículas quânticas que estão entrelaçadas de maneira que as medidas de uma partícula estejam correlacionadas com as medidas da outra, mesmo que estejam separadas por uma grande distância. Isso significa que, quando uma das partículas é medida em uma base específica, a medida da outra partícula também é determinada. Assim, para criar uma chave de criptografia compartilhada, *Alice* e *Bob* medem as partículas em suas respectivas bases escolhidas aleatoriamente. Eles então comparam as bases utilizadas e as medidas obtidas, descartando os resultados correspondentes às bases diferentes. O resultado final é uma série de bits que podem ser usados como uma chave de criptografia compartilhada, que é resistente a interceptações, pois qualquer tentativa de observar as partículas quânticas alteraria seu estado.

No E91, *Alice* não encaminha os qubits diretamente pelo canal físico entre ela e *Bob*. Para que o envio dos qubits ocorra, primeiro *Alice* cria um par entrelaçado com um nó intermediário, que deve fazer o mesmo com *Bob*. Após estabelecer essas conexões, os pares entrelaçados intermediários deixam de existir para formar apenas uma conexão direta entre *Alice* e *Bob*, por meio do processo de troca de entrelaçamento (*entanglement swapping*) [Abelém et al. 2020]. Agora *Alice* pode transferir o qubit diretamente para *Bob*, sem precisar reservar o canal para esta ação, isso torna o canal disponível para outras execuções do mesmo protocolo. Assim, a quantidade de pares EPR disponíveis no caminho entre *Alice* e *Bob* é um fator fundamental para o funcionamento do protocolo QKD E91.

3. Alocação de Recursos em Redes QKD Multiprotocolo

No contexto da rede QKD, o processo de agendamento e alocação das requisições é fundamental para garantir a entrega eficiente e segura das chaves quânticas para aplicações de segurança. Cada requisição é caracterizada por informações, como Alice e Bob, o tipo de protocolo de criptografia, a quantidade de chaves necessárias, a fidelidade miníma requerida, e o tempo máximo para atendimento (*t1*). Esse tempo máximo representa o limite em que a requisição deve ser concluída para atender às necessidades do usuário. No entanto, a alocação dessas requisições enfrenta desafios, especialmente na maximização da taxa de solicitações atendidas e na otimização da vazão da rede, considerando limitações como o tamanho da rede, a quantidade fixa de qubits e a capacidade dos canais de comunicação. Com o objetivo de melhorar esse processo, é essencial considerar não apenas o tempo para atendimento, mas também o tempo de processamento da requisição na rede (*t2*) e o tempo máximo de inicio de atendimento da requisição (*t3*), para garantir uma alocação eficiente e oportuna das requisições.

Nossa proposta visa priorizar as requisições que necessitam de atendimento ime-

diato. Para isso, propomos um algoritmo de alocação que leva em consideração todos esses critérios, apresentado no Algoritmo 1. Em caso de empate, priorizamos as requisições com (*t1*) menor, ou seja, aquelas que têm prazo de atendimento mais próximo. Em seguida, consideramos o (*t2*), que indica o tempo estimado para o processamento da requisição na rede. Além disso, para aprimorar ainda mais o processo de alocação, levamos em conta o tamanho da rota, priorizando inicialmente as rotas mais curtas. Essa abordagem busca otimizar não apenas a taxa de requisições atendidas, mas também a eficiência global da rede, garantindo que as necessidades dos usuários sejam atendidas de forma rápida e confiável.

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)
        $t3 \leftarrow r.t1 - TempoAtual$, $t2 \leftarrow 1 + \frac{r.tamanhoChaves}{N.qubits \times r.taxaSucessoProtocolo}$
        if $rota$ não está ocupada e $t3 > 0$ **then**
            Agendar r na $rota$ e **break**
        end if
    end for
    if não foi agendada **then**
        Adiar r para próxima execução
    end if
end for

4. Configuração dos Experimentos

Para avaliar o sistema proposto, foi realizado um estudo de caso com aplicações de segurança. A modelagem da arquitetura da rede e a alocação de recursos foram implementadas através de simulação discreta, utilizando a linguagem de programação Python. Os códigos desenvolvidos para o sistema, a codificação dos protocolos QKD, assim como os *scripts* específicos para a simulação do estudo de caso, estão disponíveis publicamente no repositório do artigo[1].

No âmbito desse estudo de caso, configuramos diversos cenários de aplicação. Todos esses cenários incluem 5 aplicações de segurança, cada uma com necessidades diferentes de chaves: App1 requer 100 chaves, App2 requer 200, App3 requer 500, App4 requer 1000, e App5 requer 1500. Durante os experimentos conduzidos, as requisições de chaves foram distribuídas de forma variada entre essas aplicações, seguindo proporções distintas conforme detalhado na Tabela 1.

Nesse cenário, cada requisição é caracterizada por um par único de emissor (*Alice*) e receptor (*Bob*), com a quantidade de chaves quânticas necessárias variando de acordo com a aplicação específica. Esta variação é determinada pelas exigências de segurança e autenticação de cada aplicação, o que influencia diretamente na demanda por chaves

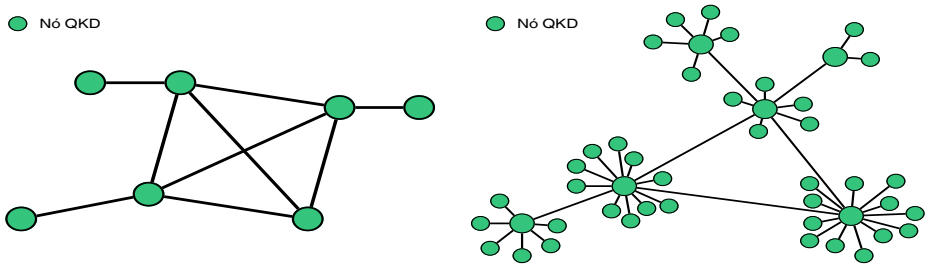
[1]https://github.com/artuenric/qkd-net

Tabela 1. Distribuição Percentual por Caso e Aplicação.

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%

quânticas. Portanto, a distribuição e o atendimento das requisições são adaptados para as necessidades específicas de segurança de cada aplicação dentro do experimento.

No estudo de caso foram utilizadas duas topologias de rede, as topologias das redes QKD reais da China e de Viena, apresentadas na Figura 2. Essas topologias foram escolhidas por representarem exemplos reais de implementações de redes QKD em ambientes de produção, oferecendo um contexto prático e relevante para a análise. Em nossa abordagem, cada nó na rede é tratado como um potencial ponto de origem ou destino para as requisições de segurança. Isso permite a avaliação do desempenho da rede sob condições variadas de tráfego e padrões de comunicação, refletindo as complexidades e desafios enfrentados em redes QKD reais.



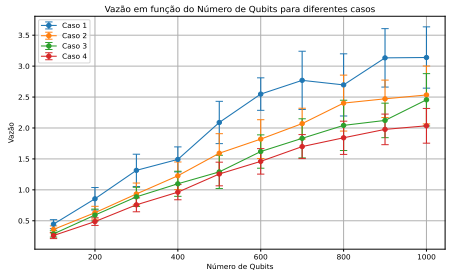
(a) Topologia da rede QKD Viena. (b) Topologia da rede QKD China.

Figura 2. Topologias das Redes QKD Utilizadas.

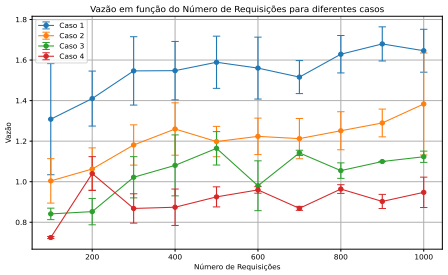
5. Resultados

Nessa Seção temos os resultados para quatro diferentes configurações de distribuição de aplicações, com os resultados sendo apresentados na Figura 3. Na Figura 3, temos que o Caso 1, caracterizado pela predominância da aplicação 1 e menor incidência das aplicações 4 e 5, apresenta um desempenho superior. Esta observação é consistente em ambas as topologias. A diferença de desempenho entre os quatro casos estudados é relativamente pequena, indicando que a presença de aplicações mais exigentes em termos de recursos (como as aplicações 4 e 5) tem um impacto significativo no desempenho global do sistema.

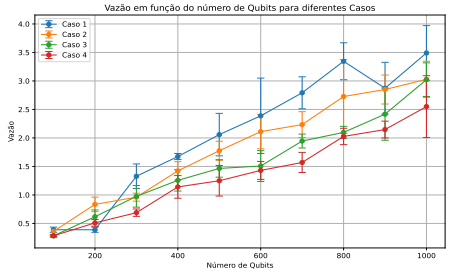
Essa tendência sugere que o balanceamento na distribuição das aplicações de segurança, priorizando aquelas que requerem menos recursos, pode ser uma estratégia eficaz para melhorar o desempenho em cenários com múltiplas aplicações. Os resultados obtidos para o Cenário 2 evidenciam a importância de uma gestão equilibrada das aplicações de segurança em sistemas de comunicação. A seleção e distribuição adequadas das



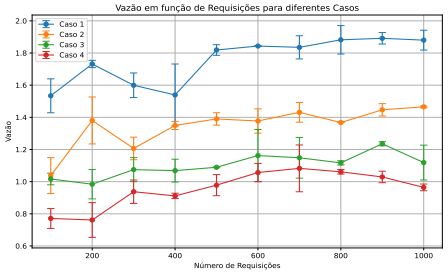
(a) Qubits Enviados - Topologia Viena.



(b) Número de Requisições - Topologia Viena.



(c) Qubits Enviados - Topologia China.



(d) Número de Requisições - Topologia China.

Figura 3. Resultados com Diferente casos de distribuição das Aplicações.

aplicações, considerando suas demandas específicas de recursos, podem ser cruciais para melhorar a eficiência e a eficácia da infraestrutura de segurança em redes de diferentes topologias, como demonstrado pelas topologias de Viena e China.

6. Conclusão e Trabalhos Futuros

Este estudo demonstrou a viabilidade e eficácia da proposta de alocação de recursos em ambientes de rede multiprotocolo. Nota-se que a gestão de recursos e a distribuição adequada das aplicações são essenciais para melhorar a vazão e a eficiência das redes QKD, pavimentando o caminho para uma Internet Quântica mais segura e eficiente.

Para trabalhos futuros, sugere-se a expansão da arquitetura para abranger uma variedade maior de cenários de aplicação e desafios de segurança. Isso inclui a integração com tecnologias emergentes de computação quântica e a exploração de novos protocolos QKD, visando aumentar a segurança e a eficiência. Além disso, um caminho também seria investigar o impacto da arquitetura em cenários de rede de grande escala e sua interação com as redes clássicas existentes, focando na 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.

Referências

Abelém, A., Vardoyan, G., and Towsley, D. (2020). Quantum internet: The future of internetworking. In *Minicursos do XXXVIII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, pages 48–90. SBC.

Abreu, D., Abelém, A., and Rothenberg, C. R. E. (2022). Desafios e oportunidades de pesquisa para o roteamento em redes quânticas. In *Anais do II Workshop de Comunicação e Computação Quântica*, pages 37–42. SBC.

Bennett, C. H. (1992). Quantum cryptography using any two nonorthogonal states. *Physical review letters*, 68(21):3121.

Bennett, C. H. and Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. *Theoretical computer science*, 560:7–11.

Cao, Y., Zhao, Y., Wang, Q., Zhang, J., Ng, S. X., and Hanzo, L. (2022a). The evolution of quantum key distribution networks: On the road to the qinternet. *IEEE Communications Surveys & Tutorials*, 24(2):839–894.

Cao, Y., Zhao, Y., Wu, Y., Yu, X., and Zhang, J. (2018). Time-scheduled quantum key distribution (qkd) over wdm networks. *Journal of Lightwave Technology*, 36(16).

Cao, Y., Zhao, Y., Zhang, J., and Wang, Q. (2022b). Software-defined heterogeneous quantum key distribution chaining: An enabler for multi-protocol quantum networks. *IEEE Communications Magazine*, 60(9):38–44.

Cao, Y., Zhao, Y., Zhang, J., Wang, Q., Niyato, D., and Hanzo, L. (2022c). From single-protocol to large-scale multi-protocol quantum networks. *IEEE Network*, 36(5):14–22.

Ekert, A. K. (1991). Quantum cryptography based on bell's theorem. *Physical review letters*, 67(6):661.

Fu, Y., Hong, Y., Quek, T. Q., Wang, H., and Shi, Z. (2020). Scheduling policies for quantum key distribution enabled communication networks. *IEEE Wireless Communications Letters*, 9(12):2126–2129.

Ribezzo, D., Zahidy, M., Vagniluca, I., Biagi, N., Francesconi, S., Occhipinti, T., Oxenløwe, L. K., Lončarić, M., Cvitić, I., Stipčević, M., et al. (2023). Deploying an inter-european quantum network. *Advanced Quantum Technologies*, 6(2):2200061.

Tavares, D., Pimentel, A., Abreu, D., and Abelém, A. (2023). Estudo e simulaçao de uma rede de distribuiçao de chaves quânticas de alto desempenho para o campus da ufpa. In *Anais da III Escola Regional de Alto Desempenho Norte 2 e III Escola Regional de Aprendizado de Máquina e Inteligência Artificial Norte 2*, pages 17–20. SBC.

Xu, F., Ma, X., Zhang, Q., Lo, H.-K., and Pan, J.-W. (2020). Secure quantum key distribution with realistic devices. *Reviews of Modern Physics*, 92(2):025002.

Yu, J., Qiu, S., and Yang, T. (2023). Optimization of hierarchical routing and resource allocation for power communication networks with qkd. *Journal of Lightwave Technology*.

Zhang, Q., Ayoub, O., Gatto, A., Wu, J., Musumeci, F., and Tornatore, M. (2023). Routing, channel, key-rate and time-slot assignment for qkd in optical networks. *IEEE Transactions on Network and Service Management*.