RanA: Uma Abordagem Híbrida para QKD BB84 com Expansão e Encapsulamento de Chave

Marcus Freire[1], Thiago Luigi Mello[1], Isys Sant'Anna [1], Adriano Maia[1], Rodrigo Moreira[2], Roberto Rivelino[3], Maycon Peixoto[1]

[1]Instituto de Computação, Universidade Federal da Bahia (UFBA)
{marcus.elias,thiagomello,isys.nogueira,adriano.maia,maycon.leone}@ufba.br

[2]Instituto de Física Gleb Wataghin, Universidade Estadual de Campinas (Unicamp)
rirm@ifi.unicamp.br

[3]Instituto de Física, Universidade Federal da Bahia (UFBA)
rivelino@ufba.br

Abstract. *Quantum cryptography, exemplified by the BB84 protocol, ensures secure key distribution through principles of quantum mechanics such as superposition and the no-cloning theorem. However, limitations in key generation rates and scalability, along with attenuation and noise in quantum channels, hinder its practical deployment in high-demand scenarios. This study proposes a hybrid approach combining BB84 with Argon2-based key derivation and Kyber512 privacy amplification, reducing dependence on quantum channels while increasing efficiency and robustness against quantum attacks. Experimental results validate the protocol's scalability and security.*

Resumo. *A criptografia quântica, exemplificada pelo protocolo BB84, permite a distribuição segura de chaves com base em princípios da mecânica quântica, como superposição e o teorema da não clonagem. Contudo, limitações na taxa de geração de chaves, escalabilidade, problemas de atenuação e ruído nos canais quânticos dificultam sua aplicação prática em cenários de alta demanda. Este estudo propõe uma abordagem híbrida que combina o BB84 com derivação de chaves baseada no Argon2 e amplificação de privacidade utilizando o Kyber512, reduzindo assim a dependência dos canais quânticos e aumentando a eficiência e a robustez contra ataques quânticos. Os resultados experimentais validam a escalabilidade e a segurança do protocolo.*

1. Introdução

A criptografia quântica é uma abordagem promissora para garantir a segurança da informação em um cenário em que tecnologias quânticas façam parte do cotidiano. Protocolos como o BB84 [Bennett and Brassard 2014] utilizam características da teoria quântica, como a superposição e o teorema da não-clonagem [Wootters and Zurek 1982], para viabilizar a distribuição segura de chaves criptográficas. Entretanto, a crescente viabilidade de computadores quânticos representa uma ameaça significativa aos sistemas de criptografia clássicos, destacando a importância de estratégias híbridas para mitigar essas vulnerabilidades [Kamel et al. 2024, Nielsen and Chuang 2010].

Embora o protocolo BB84 ofereça segurança contra *eavesdropping*, ele enfrenta limitações operacionais significativas, principalmente no que diz respeito à taxa de geração de chaves e à escalabilidade em cenários com alta demanda de tráfego seguro

[Lee et al. 2022]. *Eavesdropping* é a interceptação da transmissão quântica, onde um espião (Eva) mede os estados quânticos no canal, introduzindo alterações detectáveis nos qubits. Além disso, os canais quânticos são inerentemente suscetíveis a limitações físicas, como atenuação e ruído, que comprometem a eficiência e a viabilidade prática do protocolo em longas distâncias [Brassard et al. 2000].

Diversas abordagens têm sido propostas para melhorar a eficiência e a segurança do BB84. Entre elas, destacam-se métodos de otimização do canal quântico, integração com algoritmos de derivação de chaves e adoção de esquemas pós-quânticos. No entanto, essas soluções frequentemente apresentam desafios, como dependência de infraestrutura sofisticada, complexidade computacional e custos elevados, limitando sua aplicação prática [Rahmanpour et al. 2024, Kaur and Singh 2024, Jiang et al. 2021]. Apesar dos avanços recentes, persiste um descompasso entre as demandas por segurança em larga escala e as capacidades dos protocolos quânticos atuais. Em particular, a incapacidade de gerar chaves suficientemente longas para aplicações de alta demanda e a dependência exclusiva de canais quânticos são lacunas críticas que necessitam de abordagens inovadoras para serem superadas [Liao et al. 2022].

Dessa forma, este trabalho propõe o **RanA** (*Random Amplification*), uma abordagem híbrida que combina o protocolo BB84 com técnicas de *Key Derivation Function (KDF)* [Biryukov et al. 2016] e ampliação de privacidade utilizando o algoritmo Kyber512 [Gitonga 2025]. O objetivo é reduzir a dependência do canal quântico, aumentar a taxa de geração de chaves e viabilizar a cifragem de grandes volumes de dados. RanA integra princípios de segurança quântica com funções de derivação de chaves para expandir a chave gerada pelo BB84, enquanto o Kyber512 encapsula e protege a comunicação. As principais contribuições incluem: **(i)** a definição de um protocolo híbrido que combina segurança quântica e pós-quântica; **(ii)** a introdução de um esquema de derivação de chaves baseado no Argon2 para aumentar a entropia e a eficiência; e **(iii)** a implementação de uma ampliação de privacidade por meio do Kyber512, assegurando maior resistência contra ataques quânticos.

2. Trabalhos Relacionados

O impacto da computação quântica na criptografia clássica e a viabilidade de alternativas pós-quânticas são analisados nos trabalhos a seguir. Em [Gitonga 2025], os autores destacam as vulnerabilidades do RSA e ECC sob o algoritmo de Shor, explorando esquemas como CRYSTALS-Kyber, SPHINCS+ e McEliece. Embora destaquem o potencial dessas abordagens, também apontam desafios na escalabilidade da Distribuição Quântica de Chaves (QKD), sugerindo que abordagens híbridas podem mitigar essas limitações. Em paralelo, [Kamel et al. 2024] compara o protocolo BB84 de QKD ao Triple DES (3DES), destacando sua segurança robusta e limitações como baixa velocidade e alto custo operacional, ressaltando barreiras tecnológicas para sua adoção em larga escala.

Existem estudos de aprimoramento do protocolo BB84. O trabalho de [Lee et al. 2022] investiga a detecção de *eavesdropping* no BB84 utilizando a desigualdade de Hoeffding e algoritmos combinatórios para ajustes dinâmicos na polarização. Para garantir uma taxa de detecção de tentativas de espionagem de $99,92\%$, com falsos positivos e negativos abaixo de $0,009\%$, foi necessário manter um QBER (*Quantum Bit Error Rate*) em torno de $12,5\%$, transmitindo no mínimo 300 qubits. Esses erros são

fundamentados no fato de que para cada estado transmitido, há uma probabilidade de erro que pode ser expressa por QBER $= \frac{n_{\text{err}}}{n_{\text{det}}}$, onde n_{err} é o número de erros na detecção e n_{det} é o total de bits verificados.

Similarmente, [Rahmanpour et al. 2024] propõe uma versão aprimorada do BB84 que reduz pulsos posteriores e contagens escuras em detectores de fótons por meio de sincronização otimizada, melhorando a distribuição de chaves, mas exigindo maior quantidade de fótons de sincronização. Por outro lado, [Bhatia et al. 2025] desenvolve um protocolo BB84 otimizado para dispositivos IoT, reduzindo *overhead* em 50% via bits-chave pré-determinados e validação por hash, embora dependa de PRNG (*Pseudo-random Number Generators*) e *hardware* confiável para garantir escalabilidade.

O estudo de [Brassard et al. 2000] analisa perdas no canal, erros em detectores e limitações de pulsos fracos, sugerindo que fontes PDC (*Parametric Down-Conversion*) podem aumentar a eficiência, mas restringem a QKD a distâncias moderadas. Complementando essa abordagem, [Kaur and Singh 2024] propõe um protocolo adaptativo de QKD para redes SDN (*Software Defined Networking*), utilizando múltiplos canais para gerar chaves mais longas e resistentes a ataques, mas com maior complexidade de hardware.

Estratégias híbridas também são exploradas. O estudo de [Jiang et al. 2021] combina QKD com PRNGs clássicos, utilizando chaves geradas quanticamente como sementes para PRNGs baseados em congruência linear, equilibrando segurança e eficiência, embora dependente de infraestrutura quântica. Paralelamente, [Liao et al. 2022] avalia a segurança de protocolos quânticos, incluindo *quantum money*, VBQC (*Verifiable Blind Quantum Computation*) e assinatura digital quântica na plataforma NetSquid, destacando que a coerência da memória quântica impacta sua fidelidade, mas sua análise é limitada por parâmetros específicos de hardware.

A Tabela 1 mostra que a maioria das abordagens analisadas emprega exclusivamente QKD sem mecanismos complementares para reforço da segurança das chaves geradas. Algumas propostas incorporam derivação de chaves, mas sem considerar técnicas de segurança pós-quântica. **RanA** diferencia-se dos trabalhos analisados por combinar QKD com derivação de chaves baseada em Argon2 e amplificação de privacidade via Kyber512, mitigando as limitações do BB84 quanto à taxa de geração de chaves e escalabilidade.

Tabela 1. Comparação dos Trabalhos Relacionados

Artigos	*QKD*	*KDF*	*Pós-Quântico*	*Simulação Quântica*
[Gitonga 2025]	✓	✓	✓	-
[Lee et al. 2022]	✓	-	-	-
[Kamel et al. 2024]	✓	-	-	-
[Brassard et al. 2000]	✓	-	-	-
[Rahmanpour et al. 2024]	✓	-	-	✓
[Kaur and Singh 2024]	✓	-	✓	✓
[Bhatia et al. 2025]	✓	-	✓	-
[Jiang et al. 2021]	✓	✓	-	-
[Liao et al. 2022]	✓	-	-	✓
RanA	✓	✓	✓	✓

3. RanA: Protocolo de Ampliação de Chave Quântica

O avanço da computação quântica aumentou a demanda por protocolos de segurança para comunicações, impulsionando o desenvolvimento do QKD. Entre esses protocolos, o BB84 utiliza o teorema da não-clonagem para permitir que duas partes, Alice e Bob, estabeleçam uma chave criptográfica segura por meio de medições de qubits: por conta deste teorema, algumas tentativas de interceptação de um possível invasor alteram os estados quânticos transmitidos, o que o tornam detectável por Alice e Bob, de forma a garantir a segurança da comunicação. A Figura 1 ilustra a dinâmica desse processo.

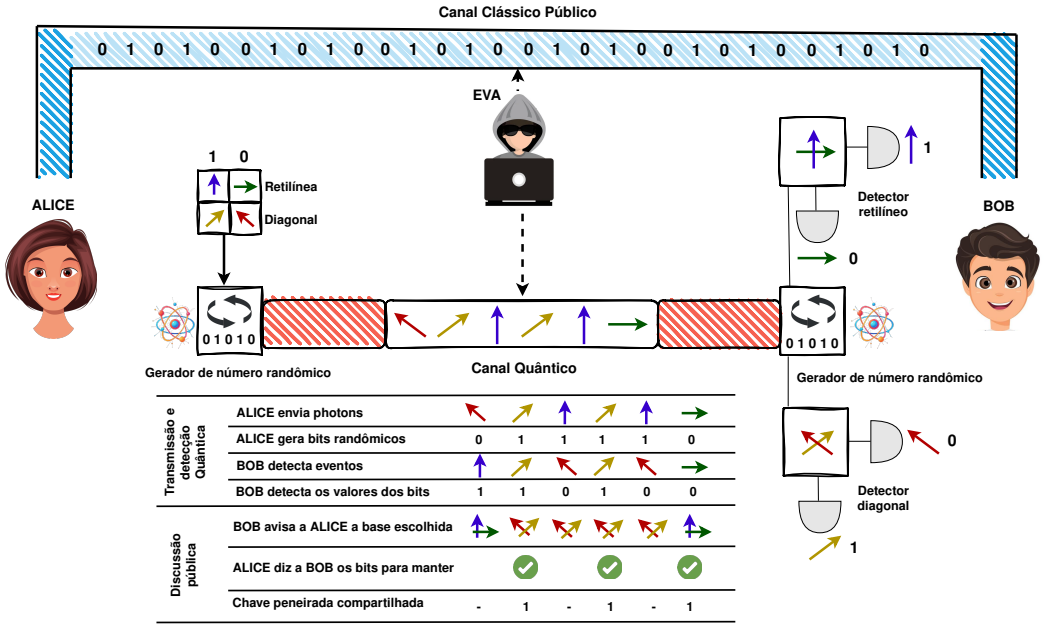


Figura 1. Esquema do protocolo BB84: Alice envia fótons polarizados aleatoriamente pelo canal quântico. Bob os mede com bases aleatórias e, na fase pública, ambos comparam bases, descartando bits incompatíveis para formar a chave. A presença de um invasor ativa os mecanismos de detecção de espionagem.

Seguindo a formulação apresentada em [Wolf 2021], assumimos que a parte quântica do protocolo BB84 é descrita pelas seguintes etapas:

1. Alice gera aleatoriamente duas sequências de bits, $a = (a_1, \ldots, a_n)$ e $c = (c_1, \ldots, c_n)$, onde a representa a string de bits que será enviada para Bob e c define a codificação quântica aplicada a cada bit de a.
2. Para cada i, se $c_i = 0$, a codificação de a_i é dada por $0 \mapsto |0\rangle \equiv (1\ 0)^T$, $\quad 1 \mapsto |1\rangle \equiv (0\ 1)^T$. Se $c_i = 1$, utiliza-se a codificação $0 \mapsto |+\rangle$, $\quad 1 \mapsto |-\rangle$, com $|\pm\rangle$ definidos conforme a eq. (3).
3. Alice transmite os qubits gerados para Bob através do canal quântico. O estado recebido pode sofrer alterações devido a ruído ou tentativas de interceptação, resultando no estado $|\psi_{a_i c_i}\rangle$, potencialmente distinto do estado originalmente enviado.
4. Bob, ao receber um qubit, escolhe aleatoriamente um bit b_i, determinando a base de medição. Se $b_i = 0$, ele realiza a medição na base computacional $(|0\rangle, |1\rangle)$:

$$M_{d_i=0|b_i=0} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad M_{d_i=1|b_i=0} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}. \tag{1}$$

Caso $b_i = 1$, a medição ocorre na base de Hadamard $(|+\rangle, |-\rangle)$:

$$M_{d_i=0|b_i=1} = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \quad M_{d_i=1|b_i=1} = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}. \tag{2}$$

5. Após a medição, Bob obtém um bit d_i, cuja distribuição de probabilidade é dada por $p(d_i|b_i, a_i, c_i) = \langle\psi_{a_i c_i}|M_{d_i|b_i}|\psi_{a_i c_i}\rangle$, obtida pelo produto interno complexo entre os vetores $|\psi_{a_i c_i}\rangle$ e $M_{d_i|b_i}|\psi_{a_i c_i}\rangle$.
6. No caso ideal, se $b_i = c_i$, então $d_i = a_i$ com probabilidade unitária. Caso contrário, d_i assume a_i com probabilidade $1/2$, pois valem as relações abaixo:

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{3}$$

$$|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle), \quad |1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle). \tag{4}$$

Para assegurar a integridade da chave gerada, Alice e Bob anunciam publicamente suas strings c e b, descartando os casos em que $c_i \neq b_i$.

A segurança do BB84 impede a replicação exata de estados quânticos sem perturbações detectáveis. Qualquer interceptação altera os estados, permitindo que Alice e Bob identifiquem um espião. Isso ocorre devido ao desconhecimento da base de polarização utilizada no envio, reduzindo a coincidência de bases para cerca de 25% em vez de 50%. Assim, a chave só é usada se sua integridade for verificada.

Para superar essa restrição, a chave bruta K gerada no BB84 passa por um processo de reconciliação para corrigir erros decorrentes de ruído no canal quântico ou tentativas de interceptação. O protocolo CASCADE é aplicado nessa etapa, permitindo que Alice e Bob obtenham uma chave corrigida K' e reduzindo discrepâncias na sequência de bits compartilhada. Para mitigar esses erros, adotamos a implementação do algoritmo CASCADE disponível em [Liao et al. 2022], que melhora a taxa de transmissão de chaves secretas em cenários com ruído e perdas. A eficiência da distribuição de chaves em fibra óptica é afetada pela taxa de defasagem, que reflete a decoerência dos qubits ao longo da transmissão.

De maneira geral, a Figura 2 ilustra o processo de distribuição e reconciliação de chaves no RanA. À esquerda, a chave gerada pelo protocolo BB84 está sujeita a ruídos e possíveis interferências durante a transmissão. O protocolo CASCADE é aplicado para corrigir erros por meio de interações sucessivas, garantindo que Alice e Bob obtenham uma chave reconciliada.

No entanto, mesmo após a aplicação do CASCADE, a taxa de geração de chaves K' no protocolo BB84 é limitada pela capacidade do canal quântico, o que restringe sua aplicação em cenários que exigem um elevado volume de tráfego seguro. Como o protocolo se fundamenta no *one-time pad*, a quantidade de dados que pode ser cifrada diretamente pelas chaves geradas é proporcional à taxa de distribuição de chaves, tornando-se um fator crítico para a escalabilidade do sistema. No intuito de transpor esse obstáculo, o RanA apresenta um esquema híbrido que combina o BB84 com técnicas de derivação de chaves e criptografia pós-quântica, reduzindo a dependência exclusiva do canal quântico e ampliando a expansibilidade do sistema sem comprometer a segurança.

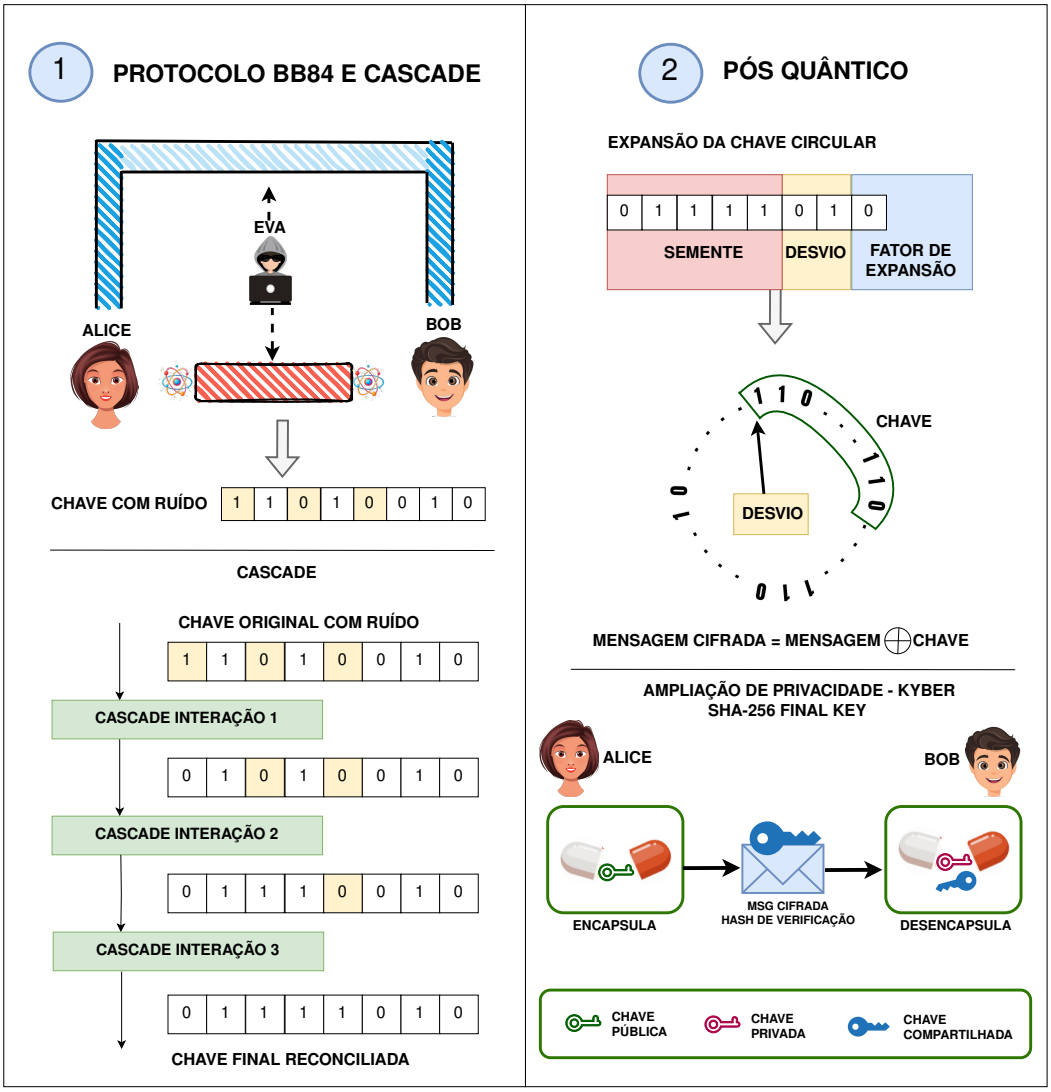


Figura 2. Esquema do RanA: à esquerda, o protocolo BB84 realiza a correção de erros via CASCADE para reconciliar a chave entre Alice e Bob. À direita, a etapa pós-quântica expande a chave e a utiliza para cifrar a mensagem, garantindo encapsulamento e integridade com Kyber512 e SHA-256.

À direita da Figura 2, a etapa pós-quântica expande a chave utilizando um fator de desvio, permitindo sua aplicação na cifragem da mensagem. A ampliação de privacidade é realizada com Kyber512, enquanto SHA-256 assegura a integridade da chave final. O encapsulamento e desencapsulamento da mensagem permitem que Alice e Bob compartilhem informações de forma segura contra ataques quânticos e clássicos.

O esquema híbrido proposto incorpora um processo de amplificação de privacidade, no qual Alice e Bob minimizam qualquer informação potencialmente acessada por Eva, assegurando que a chave final compartilhada seja segura para uso em criptografia simétrica. Além disso, a derivação de chaves possibilita a expansão da chave originalmente gerada, permitindo que o sistema proteja um volume maior de dados sem comprometer a segurança. Essa abordagem viabiliza o uso do BB84 em cenários de maior escalabilidade e resistência a ataques futuros.

O RanA é estruturada em três etapas interdependentes para ampliar a escalabilidade e a segurança do protocolo BB84. Inicialmente, a chave gerada aleatoriamente no BB84 passa por um processo de expansão, permitindo que seja utilizada de maneira eficiente em aplicações que exigem comunicação segura em larga escala. Em seguida, um mecanismo de ampliação de privacidade baseado no esquema de criptografia pós-quântica Kyber512 é aplicado, reforçando a segurança da chave contra possíveis ataques. Por fim, Bob realiza a recepção e verificação da chave expandida, assegurando sua integridade antes do uso em criptografia simétrica.

3.1. Expansão da Chave Gerada Aleatoriamente pelo BB84

A chave corrigida K' é dividida em três segmentos com proporções fixas, conforme ilustrado na Figura 2. O primeiro segmento, denominado **semente** (75%), é utilizado como entrada para a função de derivação de chave Argon2. O segundo, chamado **desvio** (15%), determina os deslocamentos aplicados durante a cifragem. Por fim, o **fator de expansão** (10%) define o tamanho final da chave expandida. A partir de K'_{seed}, aplica-se Argon2 para gerar a chave expandida K_{exp}. O tamanho da chave expandida é definido por tamanhoChaveExp $= |M| \times$ expandFactor, em que $|M|$ é o tamanho da mensagem, e expandFactor é calculado com base em K'_{numExp}.

O Argon2 é um algoritmo de derivação de chaves que permite a configuração de parâmetros como uso de memória, número de iterações e paralelismo, o que possibilita ajustá-lo a diferentes ambientes e cenários de segurança [Biryukov et al. 2016]. A função de hash subjacente é BLAKE2b, empregada para converter dados de entrada em valores de tamanho fixo, assegurando integridade. Algoritmos como bcrypt e PBKDF2 possuem menor adaptabilidade em comparação ao Argon2.

A derivação ocorre iterativamente até que o tamanho necessário seja atingido, aumentando a entropia para a cifragem. Para garantir a sincronização entre Alice e Bob, realiza-se um deslocamento circular definido por desvio $\leftarrow$ BitsParaInt$(K'_{\text{desvio}}) \bmod |K_{\text{exp}}|$, onde BitsParaInt converte os bits do segmento em um inteiro. Esse valor identifica o ponto inicial do bloco de chave utilizado na cifragem.

Alice seleciona do K_{exp} um bloco de tamanho $|M|$ para aplicar XOR à mensagem M, produzindo o texto cifrado C. Em seguida, calcula-se $\text{hash}_{\text{kyber}} = \text{SHA3-256}(K_{\text{segmento}})$, enviado a Bob para que ele valide se ambos geraram o mesmo bloco de chave. Essa etapa dificulta ataques de força bruta contra a semente e combina deslocamento e fator de expansão determinados pelo canal quântico, inviabilizando abordagens invasoras. O Algoritmo 1 apresenta a correção, expansão da chave e geração do hash de validação, etapas em comum a Alice e Bob que seguem a geração de K por meio do BB84.

3.2. Ampliação de Privacidade com Kyber512

Kyber é um algoritmo pós-quântico do processo de padronização NIST [Gitonga 2025]. Sua segurança baseia-se na dificuldade computacional do problema de *Module Learning with Errors* (MLWE), que generaliza o *Learning with Errors* (LWE) para módulos sobre anéis polinomiais finitos. Especificamente, escolhe-se um anel $\mathcal{R}_q = \mathbb{Z}_q[x] \,/\, \langle x^n+1 \rangle$ para um primo q e grau n apropriado, como $n = 256$. O objetivo é explorar a suposição de que, mesmo diante de computadores quânticos, a recuperação dos coeficientes originais

Algorithm 1 Procedimento para expansão da chave

Entradas:
K: Chave Bruta Gerada pelo BB84
L: Tamanho da Chave
Saída:
K_{segmento}: chave expandida
$hash\_key$: hash de validação da mensagem

procedure RANA(K, L)
  $K' \leftarrow \text{CASCADE}(K)$ ▷ *Correção de erros*
  $K'_{seed} \leftarrow 0.75 \times |K'|;\ K'_{desvio} \leftarrow 0.15 \times |K'|;\ K'_{numExp} \leftarrow 0.10 \times |K'|$ ▷ *Segmentação de K'*
  fatorDeExp $\leftarrow$ BitsParaInt(K'_{numExp}) % fatorDeExp $>= 1$ ▷ *Fator de Expansão*
  tamanhoChaveExp $\leftarrow L \times$ fatorDeExp
  $K_{\text{exp\_inicial}} \leftarrow \emptyset$ ▷ *Derivação da Chave Expandida (K_{exp})*
  $K_{\text{exp}} \leftarrow$ Concat(Argon2($K'_{seed}, t\_cost, m\_cost, parallelism, 256), ...$)[: tamanhoChaveExp]
  desvioMod $\leftarrow desvio \bmod |K_{\text{exp}}|$ ▷ *Cálculo do Desvio Circular*
  $K_{\text{segmento}} \leftarrow$ SegmentoDaChaveCircular($K_{\text{exp}}, desvioMod, L$)
  $hash\_key \leftarrow$ SHA3_256(K_{segmento}) ▷ *Validação e Cifragem (OTP)*
end procedure

a partir de polinômios corrompidos por ruídos é intratável. Para o Kyber512, emprega-se um módulo de dimensão $k = 2$, garantindo chaves públicas e privadas de tamanho relativamente reduzido em comparação a outros esquemas baseados em reticulados.

A geração de chaves consiste em amostrar polinômios aleatórios em $\mathcal{R}_q$ segundo distribuições centradas em zero (como gaussiana ou binomial) e em efetuar operações de multiplicação e adição polinomial com ruídos, resultando na chave pública p_k e na chave privada s_k. O encapsulamento (Kyber_Encapsulate) toma como entrada a chave pública, gera uma *ephemeral key* (chave efêmera) junto a um *ciphertext* e retorna esse par para o transmissor. O desencapsulamento (Kyber_Decapsulate) recebe o *ciphertext* e, via a chave privada, recupera a *ephemeral key*, que pode ser usada em cifragem simétrica subsequente. Esse processo confere segurança ao canal de comunicação, pois a dificuldade associada à recuperação da *ephemeral key* decorre da suposição de intratabilidade do MLWE.

No protocolo descrito, adota-se criptografia de chave pública para proteger a transmissão. A chave pública de Bob (pubKeyBob) é utilizada por Alice para cifrar o texto C por meio do encapsulamento $\text{c}_{\text{kyber}} = \text{Kyber\_Encapsulate}\big(\text{pubKeyBob}, C\big)$. Em seguida, Alice envia $\{c\_kyber, c\_hash\_kyber\}$ a Bob por um canal clássico. Caso o tamanho total da mensagem exceda 1500 bytes (MTU na Internet), torna-se necessária a geração de uma nova chave via protocolo quântico, de modo a distribuir o conteúdo em múltiplos segmentos. Para simplificar, supõe-se que o pacote de envio contém apenas *payload*. No Algoritimo 2, é demonstrado o *loop* de ação de Alice, onde se criptografa e envia partes da mensagem original por vez, até que essa seja enviada por completo.

3.3. Recepção e Verificação por Bob

Ao receber o par $\{c\_kyber, c\_hash\_kyber\}$, Bob inicialmente realiza o processo de decapsulamento, computando $C_{\text{dec}} = \text{Kyber\_Decapsulate}(\text{privKeyBob}, c_{\text{kyber}})$. Em seguida, ele recria a chave expandida K_{exp}, utilizando o mesmo conjunto de parâmetros no Argon2 e a mesma forma de segmentação aplicada por Alice durante a geração da semente.

Algorithm 2 Alice

Entradas:
M: mensagem (em bits) a ser cifrada
Saídas:
c_kyber: encapsulamento do texto cifrado C
$hash\_kyber$: hash do segmento de chave para validação
$l \leftarrow |M|$
while $l > 0$ **do**
  $K \leftarrow$ BB84(300) ▷ *Distribuição de chaves quânticas*
  $K_{segmento}, hash\_key \leftarrow$ **procedure RanA**$(K, |M|)$
  $C \leftarrow M[: 1500 \times 8] \oplus K_{\text{segmento}}$ % Cifragem OTP
  $c\_kyber \leftarrow$ Kyber_Encapsulate(pubKeyBob, C) ▷ *Encapsulamento (Kyber512) e Transmissão*
  $c\_hash\_kyber \leftarrow$ Kyber_Encapsulate(pubKeyBob, $hash\_key$)
  $M \leftarrow M[1500 \times 8 :]$
  $l \leftarrow l - |C|$
  enviar (c_kyber, c_hash_kyber)
end while

Para determinar o deslocamento circular e extrair o bloco de chave, Bob obtém $\delta = \text{BitsParaInt}(K'_{\text{desvio}}) \bmod |K_{\text{exp}}|$ e seleciona o segmento $K_{\text{segmento}} \subset K_{\text{exp}}$, cujo tamanho equivale a $|C_{\text{dec}}|$. A verificação do bloco ocorre por meio da comparação $\text{hash}_{\text{local}} = \text{SHA3-256}(K_{\text{segmento}})$ com $hash\_kyber$. Caso sejam idênticos, Bob confirma a integridade do segmento e recupera a mensagem original computando $M_{\text{recuperada}} = C_{\text{dec}} \oplus K_{\text{segmento}}$.

O protocolo minimiza a dependência do canal quântico ao aproveitar chaves corrigidas para aumentar o volume de dados cifrados em cada sessão. A utilização de uma KDF como Argon2 eleva a entropia da chave, enquanto o encapsulamento baseado em Kyber512 fornece resistência frente a ataques quânticos. A verificação por SHA3-256 preserva a integridade do processo, oferecendo sincronização entre as partes. Por fim, no Algoritimo 3, Bob realiza o decapsulamento, verifica a integridade do segmento de chave e recupera a mensagem original caso a verificação de *hash* seja bem-sucedida. Esse processo híbrido combina a segurança quântica (BB84) com a segurança pós-quântica (Kyber512), assegurando resiliência frente a ameaças clássicas e quânticas.

Algorithm 3 Bob

Entradas:
c_kyber: mensagem criptografada enviada por Alice
c_hash_kyber: comprovante Hash
$K \leftarrow$ BB84(300) ▷ *Distribuição de chaves quânticas*
$C_{\text{dec}} \leftarrow$ Kyber_Decapsulate(privKeyBob, c_kyber) ▷ *Recepção e Verificação por Bob*
$K_{segmento}, hash\_kyber\_bob \leftarrow$ **procedure RanA**$(K, |C_{dec}|)$
$hash\_kyber \leftarrow$ Kyber_Decapsulate(privKeyBob, c_hash_kyber)
if $hash\_kyber\_bob = hash\_kyber$ **then**
  $M_{\text{recuperada}} \leftarrow C_{\text{dec}} \oplus K_{\text{segmento}}$
else
  descartar % Falha de integridade
end if

4. Configuração do Ambiente e dos Experimentos

Consideramos um sistema de distribuição de chaves quânticas baseado no protocolo BB84, no qual cada qubit é preparado em um dos quatro estados possíveis, por exemplo, $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Seja $\mathcal{H}$ o espaço de Hilbert de dimensão 2 associado a cada qubit. Em um ciclo de distribuição, n qubits são transmitidos de Alice para Bob através de um canal quântico, dos quais uma fração será utilizada para verificação e detecção de espionagem, enquanto o restante comporá a chave efetiva.

O canal quântico de interesse neste trabalho é denotado por Φ_L, representa a transmissão em uma fibra óptica monomodo G.652.D de comprimento L (em km). Nessa fibra, a potência de entrada P_0 (em mW) sofre uma atenuação, resultando em uma potência de saída P (em mW). Define-se o coeficiente de atenuação em dB/km como $\alpha = \frac{10}{L}\,\log_{10}\!\left(\frac{P_0}{P}\right)$, consideramos $\alpha = 0.2$ dB/km em nossos experimentos . Além disso, o canal inclui efeitos de ruído (como decoerência e erros de detecção), de modo que, para um estado de entrada $\rho \in \mathcal{B}(\mathcal{H})$, $\Phi_L(\rho) = \mathcal{A}_L\big(\mathcal{N}(\rho)\big)$, onde $\mathcal{A}_L$ modela a atenuação e $\mathcal{N}$ descreve o ruído.

Estabelecemos a taxa de geração de chaves seguras, denotada por R_s (em bits/s). Se R_q for a taxa de transmissão quântica (qubits/s) e $f(\mathrm{QBER})$ representar o fator de eficiência relacionado aos processos de correção de erros e privacidade, então $R_s = R_q \cdot f(\mathrm{QBER})$. O fator $f(\mathrm{QBER})$ tipicamente decresce na medida em que a QBER aumenta, pois mais recursos são gastos na correção e na verificação de possíveis *eavesdroppers*. Além disso, há um limite superior $\mathrm{QBER}_{\max}$ acima do qual se assume a presença de um espião, levando à anulação da chave gerada.

Para avaliar a viabilidade do sistema, consideramos os resultados experimentais de [Wang et al. 2024], nos quais a comunicação em fibra óptica foi testada em distâncias de 20, 50 e 100 km. Foram obtidas taxas de erro de $1,12\%$, $2,04\%$ e $3,81\%$ e taxas máximas de geração de chaves seguras de 39,5 kb/s, 6,35 kb/s e 128 b/s, respectivamente. Apesar dos aprimoramentos tecnológicos, tais valores ainda se mostram insuficientes para aplicações em larga escala, que demandam velocidades da ordem de Mbps.

Utilizamos o estudo de [Liao et al. 2022], que realiza um benchmarking de protocolos de redes quânticas em cenários realistas, para identificar os requisitos mínimos diante de ruídos e imperfeições do sistema. A avaliação foi realizada na plataforma de simulação NetSquid [Coopmans et al. 2021]. O NetSquid é um simulador de redes quânticas baseado em eventos discretos, projetado para modelar desde a camada física até protocolos de controle e aplicação. Ele permite a simulação de redes quânticas complexas, como cadeias de repetidores e switches quânticos, considerando imperfeições experimentais, como decoerência e perdas em canais ópticos, contribuindo para o desenvolvimento da futura internet quântica. Além disso, auxilia na análise de protocolos de comunicação quântica, como o BB84, já implementado em fibras ópticas convencionais utilizadas por operadoras de telecomunicações [Wang et al. 2024]. A rede quântica da China [Chen et al. 2021] exemplifica a viabilidade dessa tecnologia em larga escala.

No protocolo BB84 simulado no repositório desenvolvido por [Liao et al. 2022], os autores consideraram fontes de ruído e perdas, incluindo erro em medições, perda de transmissão em fibras ópticas e erro causado pela defasagem, decorrente da decoerência quântica. Esta última representa o tempo máximo em que um qubit pode ser armazenado

antes de perder informações críticas. O erro em medições resulta de falhas nos detectores, ocasionando medições incorretas dos qubits transmitidos. A perda na transmissão por fibras ópticas foi modelada considerando a atenuação do sinal e a eficiência dos detectores. Com o aumento da distância, menos fótons chegam ao destino, reduzindo a taxa de geração de chaves secretas. Neste trabalho, utilizaremos o mesmo cenário realista validado, incorporando nossa proposta, que emprega o Argon2 para derivar a chave secreta, aumentando a taxa de dados transmitidos pelo canal clássico. Além disso, utilizaremos o algoritmo pós-quântico Kyber512 para encapsulamento da mensagem cifrada, utilizando como a ampliação da privacidade.

Adotamos o valor de 300 qubits na análise porque essa quantidade assegura uma taxa de erro quântico (QBER) dentro de limites aceitáveis, garantindo uma detecção precisa de espionagem no protocolo BB84. Essa escolha representa um equilíbrio entre segurança e eficiência, reduzindo a ocorrência de falsos positivos e negativos enquanto otimiza o uso de recursos quânticos sem comprometer a robustez do protocolo.

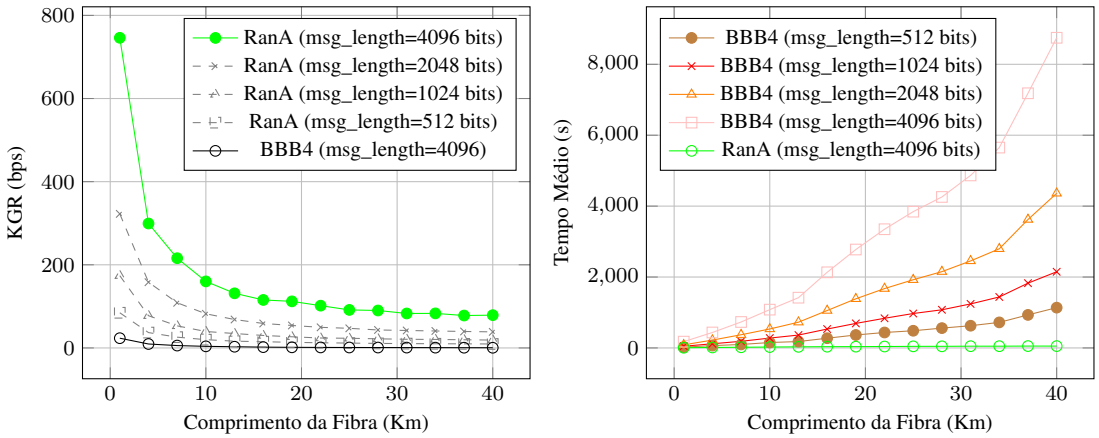
Neste trabalho, consideramos um limite de comunicação de até 40 km, um valor que, conforme indicado no no repositório desenvolvido por [Liao et al. 2022], mantém a taxa de erro em um nível aceitável após a aplicação da correção, assegurando uma comunicação quântica segura e eficiente.

5. Resultados

A Figura 3a ilustra a relação entre o comprimento da fibra óptica e a taxa de geração de chaves para diferentes tamanhos de mensagem. Observa-se que a abordagem RanA supera consistentemente o protocolo BB84 tradicional, especialmente para distâncias menores, onde a KGR atinge seu pico inicial e decai exponencialmente à medida que a atenuação óptica se intensifica. O comportamento assintótico sugere que, mesmo em distâncias mais longas, o RanA mantém uma taxa de geração de chaves superior, permitindo maior eficiência na transmissão segura de mensagens. No BB84, a necessidade de armazenamento prévio de chaves limita significativamente o desempenho, enquanto o RanA mitiga essa restrição ao empregar um esquema de derivação de chaves que reduz a dependência da taxa de geração bruta.

A Figura 3b apresenta o tempo médio necessário para a geração de chaves em função do comprimento da fibra óptica para diferentes tamanhos de mensagem. Observa-se que o protocolo BB84 tradicional apresenta um crescimento exponencial no tempo de geração de chaves, evidenciando a degradação da eficiência à medida que a distância aumenta. Esse comportamento ocorre devido à necessidade de armazenamento e reconciliação de um grande volume de chaves antes da cifragem efetiva. Em contraste, a abordagem RanA mantém um tempo de geração praticamente constante, independentemente da distância, indicando uma maior escalabilidade. Essa melhoria se deve à derivação de chaves, que reduz a dependência da taxa bruta de geração e otimiza o uso dos recursos computacionais, tornando o processo significativamente mais eficiente para aplicações de comunicação quântica em redes extensas.

A Figura 4a compara a razão de repetições necessárias no protocolo BB84 tradicional em relação à abordagem RanA para diferentes tamanhos de mensagem e distâncias na fibra óptica. Observa-se que, no BB84, o número de execuções cresce consideravelmente com o aumento da distância e do tamanho da mensagem, refletindo a ineficiência

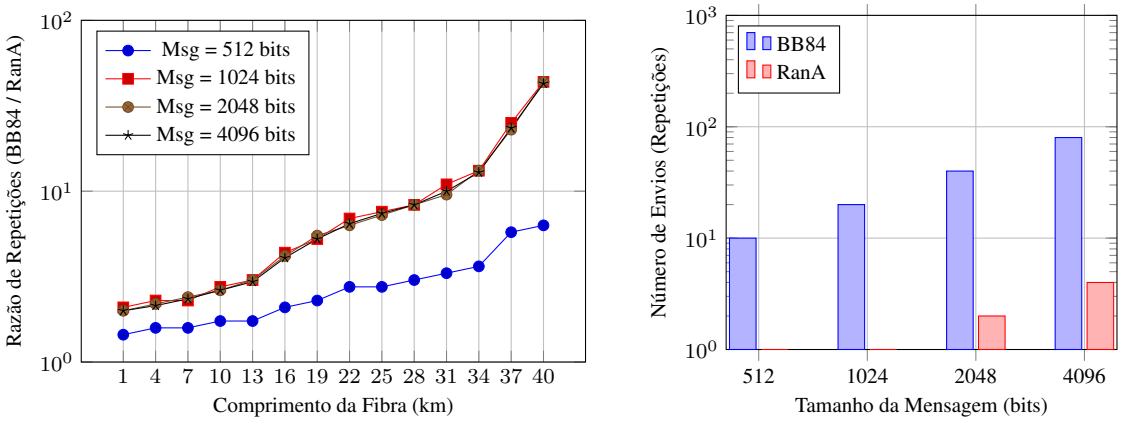


(a) Taxa de Geração de Chaves (KGR)

(b) Tempo Médio de Geração de Chaves

Figura 3. Comparação entre KGR e tempo médio de transmissão para diferentes tamanhos de mensagem.

no acúmulo de chaves antes da transmissão. Em contraste, o RanA mantém uma relação mais estável, independentemente da distância, pois a derivação da chave ocorre uma única vez. Optamos por limitar o tamanho da chave no RanA a 1024 bits, valor determinado experimentalmente para equilibrar a segurança e o desempenho, minimizando a sobrecarga computacional e melhorando a escalabilidade em redes quânticas de longa distância.



(a) Tempo médio de transmissão segura por fibra óptica.

(b) Número de Ciclos de Execuções para gerar chaves.

Figura 4. Quantidade de Envios por Tamanho de Mensagem (Escala Logarítmica)

A Figura 4b ilustra a relação entre o número de execuções do protocolo e o tamanho da mensagem para o BB84 e a abordagem RanA. Observa-se que, no BB84, o número de ciclos de execução cresce exponencialmente à medida que a mensagem se torna maior, resultando em um tempo total de transmissão significativamente elevado. Esse aumento ocorre porque a geração de chaves precisa ser repetida diversas vezes antes que a mensagem possa ser cifrada e enviada. Em contraste, o RanA reduz drasticamente esse número ao derivar a chave diretamente para o tamanho do MTU, eliminando a necessidade de múltiplas execuções para mensagens menores.

Essa otimização melhora a eficiência do protocolo ao reduzir a sobrecarga computacional, tornando a transmissão segura e escalável. Esse aspecto é relevante em sistemas que exigem segurança e eficiência na comunicação, como redes de veículos autônomos conectados, onde a distribuição de chaves deve atender a restrições de latência e integridade, conforme observado em [Peixoto 2024].

6. Conclusão

O protocolo RanA demonstrou que a combinação do BB84 com derivação de chaves via Argon2 e amplificação de privacidade com Kyber512 resulta em um esquema híbrido capaz de reduzir a dependência do canal quântico, aumentar a eficiência da distribuição de chaves e reforçar a resistência a ataques quânticos. Os experimentos validaram a escalabilidade da abordagem, evidenciando que a derivação de chaves expandidas permite cifrar maiores volumes de dados sem comprometer a segurança. Além disso, a introdução do deslocamento circular mitigou a previsibilidade no uso das chaves derivadas, dificultando ataques de correlação.

Outro aspecto relevante é a significativa redução no tempo de geração de chaves em comparação com o BB84 tradicional, que apresenta crescimento exponencial no tempo de execução conforme a distância e o tamanho da mensagem aumentam, enquanto o RanA mantém um tempo praticamente constante. Diante da evolução da computação quântica, o RanA representa um avanço para tornar a QKD viável. Sua integração com técnicas pós-quânticas fortalece a segurança do sistema contra espiões com alta capacidade computacional. Como trabalhos futuros, propõe-se a exploração de esquemas de autenticação baseados em assinaturas digitais pós-quânticas, como Dilithium, e a otimização do processo de derivação de chaves para reduzir o custo computacional.

7. Agradecimentos

Este estudo foi financiado, em parte, pela Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001, pela FAPESB, e pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), Brasil, sob a concessão nº 403231/2023-0.

Referências

Bennett, C. H. and Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7–11. Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.

Bhatia, A., Bitragunta, S., and Tiwari, K. (2025). Enhanced lightweight quantum key distribution protocol for improved efficiency and security. *IEEE Open Journal of the Communications Society*.

Biryukov, A., Dinu, D., and Khovratovich, D. (2016). Argon2: new generation of memory-hard functions for password hashing and other applications. In *2016 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 292–302. IEEE.

Brassard, G., Lütkenhaus, N., Mor, T., and Sanders, B. C. (2000). Limitations on practical quantum cryptography. *Physical review letters*, 85(6):1330.

Chen, Y.-A., Zhang, Q., Chen, T.-Y., Cai, W.-Q., Liao, S.-K., Zhang, J., Chen, K., Yin, J., Ren, J.-G., Chen, Z., et al. (2021). An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature*, 589(7841):214–219.

Coopmans, T., Knegjens, R., Dahlberg, A., Maier, D., Nijsten, L., de Oliveira Filho, J., Papendrecht, M., Rabbie, J., Rozpędek, F., Skrzypczyk, M., Wubben, L., de Jong, W., Podareanu, D., Torres-Knoop, A., Elkouss, D., and Wehner, S. (2021). Netsquid, a network simulator for quantum information using discrete events. *Communications Physics*, 4(1):164.

Gitonga, C. K. (2025). The Impact of Quantum Computing on cryptographic Systems: Urgency of Quantum-Resistant algorithms and Practical applications in cryptography. *European Journal of Information Technologies and Computer Science*, 5(1):1–10.

Jiang, Y., Liu, B., Guo, C., and Zhao, J. (2021). A quantum pseudo-random number generation scheme. *Journal of Physics: Conference Series*, 2004(1):012001.

Kamel, O. H. A., Raslan, A. T. N. E.-D., Aly, T., and Gheith, M. (2024). Quantum computing's impact on data encryption: Methodologies, implementation, and future directions: Exploring the bb84 protocol and comparative analysis with classical cryptographic techniques. In *2024 Intelligent Methods, Systems, and Applications (IMSA)*, pages 213–217. IEEE.

Kaur, H. and Singh, J. S. P. (2024). Software defined network implementation of multi-node adaptive novel quantum key distribution protocol. *AIMS Electronics & Electrical Engineering*, 8(4).

Lee, C., Sohn, I., and Lee, W. (2022). Eavesdropping detection in bb84 quantum key distribution protocols. *IEEE Transactions on Network and Service Management*, 19(3):2689–2701.

Liao, C.-T., Bahrani, S., da Silva, F. F., and Kashefi, E. (2022). Benchmarking of quantum protocols. *Scientific Reports*, 12(1):5298.

Nielsen, M. A. and Chuang, I. L. (2010). *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge ; New York, 10th anniversary ed edition.

Peixoto, M. L. M. (2024). Quantum edge computing for data analysis in connected autonomous vehicles. In *2024 IEEE Symposium on Computers and Communications (ISCC)*, pages 1–6. IEEE.

Rahmanpour, M., Erfanian, A., Afifi, A., Khaje, M., and Fahimifar, M. H. (2024). A new quantum key distribution protocol to reduce afterpulse and dark counts effects. *Results in Optics*, page 100718.

Wang, J., Rollick, B. J., Jia, Z., and Huberman, B. A. (2024). Time-interleaved c-band co-propagation of quantum and classical channels. *Journal of Lightwave Technology*, 42(11):4086–4095.

Wolf, R. (2021). *Quantum Key Distribution: An Introduction with Exercises*, volume 988 of *Lecture Notes in Physics*. Springer, 1 edition.

Wootters, W. K. and Zurek, W. H. (1982). A single quantum cannot be cloned. *Nature*, 299(5886):802–803.