Revista Eletrônica de Iniciação Científica em Computação, 2026, 24:1
ISSN: 3085-8461 • doi: 10.5753/reic.2026.8121

Artigo de Pesquisa

Distribuição de Chaves Quânticas com BB84: simulação e análise do QBER com Qiskit

Quantum Key Distribution with BB84: simulation and QBER analysis using Qiskit

Luiza Faria Petenazzi [Instituto de Tecnologia e Liderança | *luiza.petenazzi@sou.inteli.edu.br*]
Victor Takashi Hayashi [Universidade de São Paulo |*victor.hayashi@usp.br*]

Instituto de Tecnologia e Liderança, Av. Prof. Almeida Prado, 520 - Butantã, São Paulo - SP, 05508-070, Brasil.

Resumo. A computação quântica impõe desafios à segurança dos sistemas criptográficos clássicos, motivando o uso de abordagens como a Distribuição de Chaves Quânticas (QKD). Este trabalho analisa o protocolo BB84 por meio de simulação computacional, investigando a relação entre a taxa de interceptação e o Quantum Bit Error Rate (QBER). Os resultados indicam um aumento progressivo do QBER conforme cresce a interceptação, com convergência para aproximadamente 25% em cenários de interceptação total. Observa-se ainda que níveis intermediários já comprometem a segurança da chave. O estudo sugere a eficácia do QBER como indicador de interferências no contexto simulado e contribui com uma abordagem reprodutível para análise de protocolos de QKD. O código-fonte adaptado e utilizado na simulação está disponível publicamente em: `https://github.com/lupetenazzi/quantum-cryptography-bb84`

Abstract. Quantum computing challenges the security of classical cryptographic systems, motivating the adoption of approaches such as Quantum Key Distribution (QKD). This work analyzes the BB84 protocol using simulation, focusing on the relationship between interception rate and the Quantum Bit Error Rate (QBER). Results show a progressive increase in QBER as interception grows, approaching the theoretical limit of 25% under full interception. Intermediate levels are sufficient to compromise key security. The study suggests QBER as a promising indicator of eavesdropping within the simulated context and provides a reproducible approach for analyzing QKD protocols. The simulation source code is publicly available at: `https://github.com/lupetenazzi/quantum-cryptography-bb84`.

Palavras-chave: Criptografia Quântica, Distribuição de Chaves Quânticas, BB84, QBER, Simulação, Segurança da Informação

Keywords: Quantum Cryptography, Quantum Key Distribution, BB84, QBER, Simulation, Information Security

Recebido/Received: 28 April 2026 • **Aceito/Accepted:** 17 July 2026 • **Publicado/Published:** 14 August 2026

1 Introdução

O avanço da computação quântica tem levantado preocupações significativas quanto à segurança dos sistemas criptográficos tradicionais. Algoritmos amplamente utilizados, como RSA (*Rivest-Shamir-Adleman*) e ECC (*Elliptic Curve Cryptography* — Criptografia de Curva Elíptica), baseiam-se em problemas matemáticos considerados computacionalmente intratáveis para computadores clássicos, mas que podem ser resolvidos de forma eficiente por algoritmos quânticos, como o algoritmo de Shor [Shor, 1994]. Esse cenário motiva a busca por alternativas capazes de garantir segurança mesmo diante de adversários com capacidade quântica.

Nesse contexto, a criptografia quântica surge como uma abordagem promissora, explorando princípios fundamentais da mecânica quântica para garantir a segurança da informação. Em particular, a Distribuição de Chaves Quânticas (*Quantum Key Distribution* – QKD) permite a geração de chaves criptográficas com segurança baseada em leis físicas, em vez de suposições computacionais [Bennett and Brassard, 2014]. O protocolo BB84, proposto por Bennett e Brassard em 1984, é o esquema de QKD mais conhecido e estabelece um método para detecção de interceptações por meio da análise da Taxa de Erro Quântico de Bits (*Quantum Bit Error Rate* — QBER). De forma intuitiva, o QBER representa a proporção de bits que chegam com erro ao receptor após a transmissão: quanto maior essa taxa, maior a suspeita de que alguém tentou interceptar a comunicação.

Diversos trabalhos na literatura investigam tanto a implementação quanto a segurança de protocolos de QKD. Estudos como [Carrera-Rivera *et al*., 2022] discutem metodologias para análise sistemática na área de computação, enquanto abordagens práticas utilizando simuladores quânticos têm sido exploradas para avaliar o comportamento do protocolo BB84 em diferentes cenários [Combarro and González-Castillo, 2025]. Além disso, pesquisas recentes analisam o impacto de ataques do tipo *intercept-resend* — nos quais um adversário intercepta os qubits transmitidos, realiza uma medição e os reenvia ao destinatário — no aumento do QBER e na consequente detecção de intrusos [Moizuddin *et al*., 2017]. No entanto, observa-se que muitos desses estudos envolvem ambientes experimentais de maior complexidade.

Diante disso, este trabalho tem como objetivo analisar o comportamento do protocolo BB84 por meio de simulação computacional, com foco na relação entre a taxa de interceptação e o QBER. A abordagem adotada prioriza a reprodutibilidade dos experimentos e a simplicidade do ambiente de simulação, permitindo a análise do comportamento fundamental do protocolo sem a necessidade de infraestrutura avançada. Ressalta-se que os parâmetros utilizados representam uma escolha metodológica deliberada, suficiente para a observação das tendências esperadas sem necessidade de

amostras de maior escala.

Como principais contribuições, este trabalho apresenta:

Contribuição	Descrição
(i)	Implementação do protocolo BB84 em ambiente simulado utilizando ferramentas acessíveis, com o código-fonte utilizado disponibilizado publicamente
(ii)	Modelagem de um ataque do tipo *intercept-resend* com diferentes níveis de intensidade
(iii)	Análise experimental da variação do QBER em função da taxa de interceptação
(iv)	Comparação entre os resultados obtidos e o comportamento teórico esperado

Tabela 1. Principais contribuições do trabalho

Os resultados obtidos em ambiente simulado indicam que o protocolo apresenta capacidade de detectar interferências no canal quântico, sugerindo sua relevância como abordagem complementar no contexto das ameaças impostas pela computação quântica.

Por fim, este artigo está organizado da seguinte forma: a Seção 2 apresenta a fundamentação teórica sobre criptografia quântica e o protocolo BB84; a Seção 3 descreve a metodologia adotada e o ambiente de simulação utilizado; a Seção 4 apresenta os resultados experimentais e a análise do QBER em diferentes cenários de interceptação; e a Seção 5 apresenta as considerações finais e perspectivas para trabalhos futuros.

2 Fundamentação Teórica

O desenvolvimento deste trabalho está fundamentado em conceitos provenientes da criptografia clássica e da mecânica quântica, os quais, quando combinados, dão origem aos protocolos de distribuição de chaves quânticas. Esta seção apresenta os principais conceitos necessários para a compreensão do problema investigado, estabelecendo uma progressão que parte dos fundamentos da segurança da informação até a análise específica do protocolo BB84 e da métrica QBER.

2.1 Criptografia e Segurança

A criptografia é uma das principais ferramentas utilizadas para garantir a segurança da informação em sistemas computacionais. Seu objetivo é proteger dados contra acessos não autorizados, assegurando três propriedades fundamentais: confidencialidade (garantia de que a informação é acessível apenas a quem tem autorização), integridade (garantia de que os dados não foram alterados sem consentimento) e autenticidade (garantia de que as partes da comunicação são quem afirmam ser) [Forouzan, 2007]. Em aplicações práticas, a criptografia é amplamente utilizada em comunicações digitais, armazenamento de dados e sistemas distribuídos.

A Figura 1 ilustra o modelo básico de uma comunicação criptografada. Nesse modelo, Alice deseja enviar uma mensagem M a Bob de forma segura. Para isso, um Cifrador utiliza uma chave K, gerada pelo Gerador de chaves, para transformar a mensagem original em uma mensagem cifrada S, transmitida pelo canal público. Do lado de Bob, um Decifrador utiliza a mesma chave K, recebida pelo canal seguro, para recuperar a mensagem original.

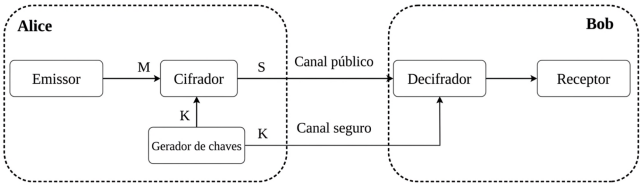

Figura 1. Modelo básico de comunicação criptografada entre Alice e Bob. Fonte: adaptado de Diamanti [2006]

Esse fluxo evidencia o papel central da chave criptográfica: sem ela, a mensagem cifrada interceptada por um adversário no canal público permanece ilegível [Diamanti, 2006]. O modelo ilustrado corresponde à criptografia simétrica, na qual a mesma chave é utilizada para cifrar e decifrar a mensagem. Diferentemente, a criptografia assimétrica, como o RSA, emprega pares de chaves distintas, dispensando o compartilhamento prévio de um segredo entre as partes.

Os sistemas criptográficos clássicos são baseados em problemas matemáticos considerados difíceis de serem resolvidos com os recursos computacionais disponíveis. Exemplos incluem a fatoração de números inteiros grandes e o cálculo de logaritmos discretos [Stallings, 2006]. A segurança desses sistemas depende da suposição de que tais problemas não podem ser resolvidos em tempo viável por um adversário.

Entretanto, essa noção de segurança é condicional, ou seja, depende diretamente das limitações dos atacantes. Com o avanço tecnológico e o surgimento de novos paradigmas, essas premissas podem deixar de ser válidas, comprometendo a segurança dos sistemas existentes. Nesse contexto, torna-se necessário analisar como novos modelos computacionais impactam a criptografia clássica.

2.2 Limitações da Criptografia Clássica frente à Computação Quântica

A computação quântica introduz um novo modelo de processamento de informação baseado em princípios da mecânica quântica, como superposição e emaranhamento. Diferentemente dos computadores clássicos, que operam com bits binários (0 ou 1), computadores quânticos utilizam qubits, que podem representar múltiplos estados simultaneamente — o que permite processar um volume muito maior de possibilidades em paralelo [Nielsen and Chuang, 2010].

Esse modelo possibilita o desenvolvimento de algoritmos capazes de resolver determinados problemas com eficiência significativamente superior à dos algoritmos clássicos. Um dos exemplos mais relevantes é o algoritmo de [Shor, 1994], que permite a fatoração de números inteiros em tempo polinomial. Como consequência, sistemas criptográficos baseados nesse problema, como o RSA, tornam-se vulneráveis em um cenário onde computadores quânticos de grande escala estejam disponíveis.

Outro exemplo é o algoritmo de [Grover, 1996], que oferece uma aceleração quadrática na busca em espaços não estruturados, impactando diretamente a segurança de algoritmos simétricos ao reduzir efetivamente o espaço de chaves necessário para manter o mesmo nível de segurança.

Diante dessas limitações, surge a necessidade de desenvolver mecanismos criptográficos que não dependam exclusivamente de suposições computacionais, mas que sejam seguros mesmo diante de adversários com capacidades quânticas [Azevedo *et al*., 2025]. É nesse contexto que a criptografia quântica se destaca como uma alternativa promissora.

2.3 Criptografia Quântica

A criptografia quântica utiliza propriedades fundamentais da mecânica quântica para garantir a segurança da informação. Diferentemente da criptografia clássica, cuja segurança depende da dificuldade computacional de certos problemas, a criptografia quântica baseia-se em leis físicas, proporcionando um nível de segurança potencialmente incondicional [Hayashi *et al*., 2025].

Entre os princípios que sustentam essa abordagem, destacam-se o princípio da incerteza de Heisenberg e o teorema da não-clonagem [Nielsen and Chuang, 2010]. O primeiro estabelece que medir certas propriedades de um sistema quântico altera inevitavelmente seu estado, ou seja, observar um qubit interfere nele. O segundo afirma que não é possível copiar um estado quântico desconhecido de forma perfeita, o que inviabiliza estratégias de espionagem baseadas em cópia silenciosa de informação.

Essas características implicam que, em condições ideais, tentativas de interceptação de uma comunicação quântica tendem a introduzir perturbações detectáveis [Hayashi *et al*., 2025]. Essa propriedade é explorada em protocolos de distribuição de chaves quânticas, permitindo que as partes envolvidas identifiquem a presença de um adversário.

Vale destacar que, no cenário atual, a principal resposta da indústria às ameaças quânticas é a criptografia pós-quântica, baseada em algoritmos clássicos resistentes a ataques quânticos e padronizada pelo NIST [National Institute of Standards and Technology, 2024]. O QKD, por sua vez, representa uma abordagem complementar, cuja segurança é fundamentada em princípios físicos em vez de suposições computacionais [Silva *et al*., 2025].

2.4 Distribuição de Chaves Quânticas (QKD)

A Distribuição de Chaves Quânticas (*Q*uantum Key Distribution — QKD) é uma aplicação direta dos princípios da criptografia quântica, permitindo que duas partes - tradicionalmente denominadas Alice (emissora) e Bob (receptor) — estabeleçam uma chave secreta compartilhada de forma segura, mesmo na presença de um possível adversário [Silva *et al*., 2025].

O funcionamento do QKD baseia-se na transmissão de informações codificadas em estados quânticos, geralmente utilizando fótons Rusca *et al*. [2018]. Durante esse processo, qualquer tentativa de interceptação por parte de um adversário (convencionalmente chamado de Eve, do inglês *eavesdropper*) implica a realização de medições sobre os estados quânticos, o que tende a alterar suas propriedades e introduzir erros detectáveis [Zhang *et al*., 2025].

Após a transmissão, Alice e Bob realizam etapas adicionais, como reconciliação de bases e verificação de erros, com o objetivo de garantir a consistência da chave gerada. Caso a taxa de erro observada seja superior a um determinado limiar, a chave é descartada, pois isso indica a possível presença de um adversário ou ruído excessivo no canal [Lee *et al*., 2022].

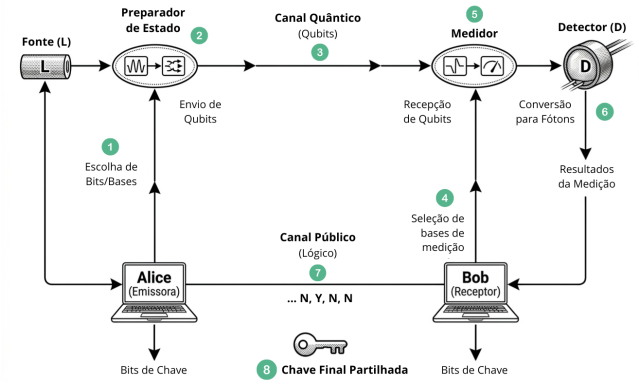

Figura 2. Fluxo do protocolo de Distribuição de Chaves Quânticas (QKD). Fonte: adaptado de Hayashi *et al*. [2025]

Conforme ilustrado na Figura 2, Alice codifica a informação em estados quânticos e os transmite a Bob por meio de um canal quântico. Um canal clássico convencional, sem propriedades quânticas, é utilizado posteriormente para que ambos comparem as bases de medição utilizadas. Caso Eve tente interceptar os qubits em trânsito no canal quântico, ela é obrigada a realizar medições, o que, pelas propriedades da mecânica quântica, altera os estados transmitidos e introduz inconsistências detectáveis entre os dados de Alice e Bob. A Figura 2 ilustra, portanto, não apenas o fluxo de comunicação, mas o mecanismo fundamental pelo qual a segurança do protocolo é sustentada, em condições ideais de implementação.

Dentre os diversos protocolos de QKD propostos na literatura, o BB84 destaca-se como o mais simples e amplamente estudado, sendo frequentemente utilizado como base para análises teóricas e experimentais.

2.5 Protocolo BB84

O protocolo BB84, proposto por Bennett e Brassard em 1984 [Bennett and Brassard, 2014], é considerado o primeiro protocolo de distribuição de chaves quânticas e um dos mais estudados [Djordjevic, 2025]. Sua simplicidade conceitual e robustez tornam-no uma referência fundamental na área.

No BB84, Alice codifica bits clássicos em estados quânticos utilizando duas bases de medição distintas: a base computacional (Z), que corresponde aos estados $|0\rangle$ e $|1\rangle$, e a base diagonal (X), que corresponde às superposições $|+\rangle$ e $|\rangle$. Para cada bit a ser transmitido, Alice escolhe aleatoriamente uma dessas bases e prepara o qubit correspondente. Bob, ao receber cada qubit, também escolhe aleatoriamente uma das duas bases para realizar sua medição.

Após a transmissão, Alice e Bob comunicam publicamente quais bases foram utilizadas em cada posição, sem comunicar os valores dos bits, e descartam todos os bits em que as bases não coincidem. Esse processo é conhecido como *sifting* (filtragem) e resulta em uma sequência de bits potencialmente compartilhada entre as partes. Em média, metade dos bits é descartada nessa etapa, pois a probabilidade de Alice e Bob escolherem a mesma base por acaso é de 50%.

A segurança do protocolo está fundamentada no fato de que um adversário não conhece previamente qual base Alice utilizou em cada qubit. Caso Eve tente interceptar a comuni-

cação e escolha uma base incorreta — o que ocorre em 50% das tentativas — o estado do qubit é perturbado, introduzindo erros na sequência de bits que podem ser detectados por Alice e Bob durante a etapa de verificação [Kumar and Mondal, 2025].

Essa capacidade de detecção é central para o funcionamento do BB84 e está diretamente relacionada à métrica QBER, detalhada a seguir.

2.6 Quantum Bit Error Rate (QBER)

O *Quantum Bit Error Rate* (QBER) é a principal métrica utilizada para avaliar a segurança e a qualidade do canal em protocolos de Distribuição de Chaves Quânticas [Djordjevic, 2025]. Ele representa a proporção de bits que chegam com erro ao receptor em relação ao total de bits comparados após o processo de *sifting* [Muga *et al*., 2011]. De forma intuitiva, o QBER funciona como um termômetro do canal quântico: em condições ideais, sem ruído ou interferência, ele deve ser nulo; qualquer desvio acima de zero indica anomalias que podem ser causadas por ruído físico ou pela presença de um adversário [Yuen, 2012].

Formalmente, o QBER pode ser definido como:

$$QBER = \frac{N_{erros}}{N_{total}} \tag{1}$$

onde N_{erros} corresponde ao número de bits divergentes entre as sequências de Alice e Bob, e N_{total} representa o número total de bits comparados após o *sifting*.

No cenário de um ataque do tipo *intercept-resend*, o adversário intercepta qubits e os remede em bases escolhidas aleatoriamente. Quando a base escolhida por Eve difere da utilizada por Alice, o que ocorre em 50% dos casos, há uma probabilidade de 50% de que o qubit reenviado cause um erro na medição de Bob. Combinando essas probabilidades e considerando a etapa de *sifting*, o valor esperado do QBER em um cenário de interceptação total converge para aproximadamente 25%, valor amplamente utilizado na literatura como referência para detecção de ataques no protocolo BB84 [Lee *et al*., 2022].

Essa relação entre interceptação e aumento do QBER torna essa métrica fundamental tanto para a detecção de ataques quanto para a avaliação da segurança do canal. Na prática, valores de QBER superiores a aproximadamente 11% são considerados indicativos de comprometimento da comunicação, levando ao descarte da chave [Lee *et al*., 2022]. Neste trabalho, o QBER será utilizado como principal indicador para analisar o impacto de diferentes níveis de interceptação em ambiente de simulação.

2.6.1 Relação entre QBER e Taxa de Interceptação

Para quantificar a intensidade de um ataque, define-se o parâmetro α como a fração de *qubits* interceptados durante a transmissão, assumindo valores entre 0 (nenhuma interceptação) e 1 (interceptação total do canal).

Como cada qubit interceptado tem, em média, 25% de chance de introduzir um erro após o *sifting*, o QBER esperado pode ser aproximado por:

$$QBER \approx 0.25 \cdot \alpha \tag{2}$$

Essa relação indica que o QBER cresce proporcionalmente à intensidade do ataque, fornecendo a base teórica para comparação com os resultados experimentais apresentados na Seção 4.

3 Metodologia

Esta seção descreve os procedimentos adotados para a implementação e análise do protocolo BB84 em ambiente simulado. O foco principal consiste na avaliação do comportamento do Quantum Bit Error Rate (QBER) sob diferentes níveis de interceptação, utilizando uma abordagem experimental baseada em simulação computacional.

A metodologia foi estruturada de forma a garantir clareza na reprodução dos experimentos, bem como alinhamento entre os conceitos teóricos apresentados e sua aplicação prática.

3.1 Ambiente de Simulação

A implementação dos experimentos foi realizada em linguagem Python, utilizando a biblioteca Qiskit [IBM Quantum, 2023], uma plataforma de código aberto amplamente empregada para o desenvolvimento e a simulação de circuitos quânticos. Como ponto de partida, a implementação foi inspirada no exemplo prático de simulação do protocolo BB84 desenvolvido por [Kejvi, 2023], disponível publicamente, e adaptada para os objetivos deste trabalho. O código original contemplava as etapas básicas do protocolo, incluindo a geração dos bits e bases de Alice, a preparação e medição dos qubits e o processo de reconciliação das bases. A partir dessa estrutura, foram incorporados o cálculo da taxa de erro quântico (QBER) e a simulação de cenários com interceptação parcial por Eve, permitindo avaliar o impacto de diferentes níveis de espionagem sobre a segurança da chave gerada. O ambiente adotado permite modelar sistemas quânticos de forma acessível, viabilizando a análise de protocolos como o BB84 sem a necessidade de hardware quântico físico [Combarro and González-Castillo, 2025].

As simulações foram executadas por meio de um simulador baseado em circuitos quânticos, no qual cada qubit é representado individualmente. Esse modelo permite observar diretamente o impacto das operações quânticas e medições no estado do sistema.

A escolha por um ambiente de simulação controlado possibilita a eliminação de variáveis externas, como ruído físico de dispositivos reais, concentrando a análise no comportamento intrínseco do protocolo. Ainda assim, o número de qubits e execuções realizadas foi definido como uma escolha metodológica deliberada, aspecto detalhado na Seção 4.

3.2 Implementação do Protocolo BB84

A implementação do protocolo BB84 foi realizada com base na modelagem clássica de três entidades: Alice (emissor), Bob (receptor) e Eve (possível adversário). Cada execução do protocolo consiste na transmissão de uma sequência de qubits preparados e medidos de acordo com bases escolhidas aleatoriamente.

Inicialmente, Alice gera duas sequências aleatórias: uma correspondente aos bits a serem transmitidos e outra correspondente às bases de codificação, escolhidas entre as bases Z e X. A preparação dos qubits é realizada aplicando operações quânticas equivalentes às escolhas de bits e bases, utilizando

portas como X e H. Bob, por sua vez, realiza medições sobre os qubits recebidos, também escolhendo aleatoriamente entre as bases Z e X. As medições são realizadas individualmente para cada qubit, refletindo o comportamento do protocolo em um canal quântico idealizado.

Após a etapa de transmissão, ocorre o processo de reconciliação de bases, conhecido como *sifting*. Nesse processo, Alice e Bob comparam publicamente as bases utilizadas e descartam todos os bits cujas bases não coincidem. O resultado dessa etapa é uma chave filtrada, potencialmente compartilhada entre as partes [Pathare *et al*., 2025].

A partir dessa chave, torna-se possível calcular o QBER, permitindo a análise da consistência da comunicação e a detecção de possíveis interferências.

3.3 Modelagem de Interceptação

A presença de um adversário foi modelada por meio de um ataque do tipo *intercept-resend*. Nesse modelo, Eve intercepta uma fração dos qubits transmitidos, realiza medições em bases escolhidas aleatoriamente e, em seguida, reenvia novos qubits para Bob com base nos resultados obtidos.

A interceptação é controlada por um parâmetro que define a fração de qubits interceptados em cada execução. Esse parâmetro varia entre 0 e 1, permitindo simular diferentes níveis de interferência no canal quântico.

Durante a interceptação, a escolha de bases por parte de Eve é independente das escolhas realizadas por Alice. Quando as bases não coincidem, a medição realizada por Eve altera o estado do qubit, introduzindo inconsistências que podem ser detectadas posteriormente por meio do aumento do QBER.

Esse modelo de ataque foi escolhido por sua simplicidade e por representar um cenário clássico de análise em protocolos de QKD, sendo amplamente utilizado na literatura para avaliar a robustez do BB84 [Djordjevic, 2025].

3.4 Definição dos Experimentos

Os experimentos foram estruturados com o objetivo de analisar o comportamento do protocolo em diferentes condições de interceptação. Dois cenários principais foram considerados.

No primeiro cenário, o protocolo é executado sem a presença de adversário, permitindo observar o comportamento ideal do sistema. Espera-se, nesse caso, que o QBER seja próximo de zero, indicando ausência de erros no processo de transmissão e medição.

No segundo cenário, são introduzidos diferentes níveis de interceptação, variando a fração de qubits interceptados. Para cada nível, múltiplas execuções independentes são realizadas, permitindo a obtenção de valores médios e desvios padrão do QBER.

Os parâmetros utilizados nas simulações foram definidos como uma escolha metodológica deliberada, visando equilibrar clareza analítica e qualidade dos resultados. Cada execução do protocolo envolveu a transmissão de 200 qubits, e para cada nível de interceptação foram realizadas 50 execuções independentes, totalizando 250 simulações ao longo de todos os cenários avaliados. Esses valores mostraram-se suficientes para evidenciar o comportamento esperado do protocolo, especialmente no que diz respeito à relação entre interceptação e aumento do QBER, conforme evidenciado pela consistência das tendências observadas.

4 Reprodutibilidade e Limitações

A metodologia foi concebida com foco na reprodutibilidade dos experimentos. A utilização de ferramentas amplamente disponíveis (Python e Qiskit) permite que os experimentos sejam replicados em hardware convencional sem dependência de infraestrutura especializada. Todo o código-fonte utilizado e desenvolvido neste trabalho, incluindo os scripts de simulação, as dependências do ambiente e as instruções de execução, está disponibilizado publicamente no repositório indicado na seção de Disponibilidade de dados e materiais.

Os parâmetros experimentais, como número de qubits, número de execuções e taxa de interceptação, podem ser ajustados diretamente no código, permitindo a replicação exata dos cenários analisados ou a exploração de novas configurações.

As simulações foram executadas em ambiente local, com a seguinte configuração de hardware: modelo Dell Latitude 3440, processador Intel Core i5-1335U de 13ª geração (12 núcleos), 16 GB de memória RAM e sistema operacional Ubuntu 24.04.4 LTS (64 bits). Essa configuração, embora adequada para os objetivos deste trabalho, impõe restrições relevantes ao escopo dos experimentos. Vale destacar que, no caso específico do BB84, cada qubit é processado individualmente e de forma não entrelaçada, de modo que o custo computacional da simulação não apresenta crescimento exponencial.

Os parâmetros adotados — 200 qubits por execução e 50 repetições por cenário — constituem uma escolha metodológica deliberada, suficiente para capturar o comportamento fundamental do protocolo, conforme evidenciado pela consistência das tendências observadas. O tempo médio de execução por cenário sem interceptação foi de aproximadamente 5 segundos, enquanto os cenários com interceptação total demandaram em média 20 minutos, ambos medidos no hardware descrito. Esses valores sugerem a viabilidade da abordagem em hardware convencional, sem dependência de infraestrutura especializada, dentro do escopo dos parâmetros adotados.

Além das limitações computacionais, é importante destacar que simuladores quânticos clássicos não reproduzem integralmente os efeitos físicos presentes em hardware quântico real, como ruído de canal, decoerência e perdas ópticas. Os resultados obtidos representam, portanto, uma aproximação do comportamento ideal do protocolo BB84, adequada para análise conceitual e validação do modelo, mas não substituindo experimentos conduzidos em dispositivos quânticos reais. Ainda assim, as tendências observadas são consistentes com o comportamento teórico esperado, reforçando a validade da abordagem adotada dentro do escopo proposto.

5 Resultados Experimentais

Esta seção apresenta os resultados obtidos a partir da simulação do protocolo BB84 em diferentes cenários experimentais. Os experimentos foram organizados de forma a avaliar tanto o comportamento ideal do protocolo quanto seu desempenho sob a presença de interceptação.

Para cada cenário, foram realizadas múltiplas execuções independentes, permitindo a análise do valor médio do QBER e sua variabilidade por meio do desvio padrão associado.

5.1 Experimento 1: Cenário sem Interceptação

O primeiro experimento teve como objetivo avaliar o comportamento do protocolo BB84 em um ambiente ideal, sem a presença de um adversário. Nesse cenário, Alice e Bob realizam o processo completo de transmissão, medição e reconciliação de bases, sem qualquer interferência externa.

Os resultados obtidos indicam que o QBER permaneceu igual a zero em todas as execuções realizadas. Esse comportamento reflete a ausência de perturbações no canal quântico, garantindo total consistência entre as chaves obtidas por Alice e Bob após o processo de *sifting*.

Além disso, observou-se que aproximadamente metade dos bits transmitidos foi descartada durante a etapa de reconciliação de bases, resultado esperado devido à escolha aleatória das bases por ambas as partes. Esse comportamento confirma a correta implementação do protocolo, uma vez que a taxa de aproveitamento da chave está alinhada com o comportamento teórico do BB84.

5.2 Experimento 2: Cenário com Interceptação

O segundo experimento analisou o impacto da presença de um adversário no canal quântico, modelado por meio de um ataque do tipo *intercept-resend*. Foram considerados diferentes níveis de interceptação, variando a fração de qubits interceptados ao longo das execuções.

Para cada nível de interceptação, foram realizadas 50 execuções independentes, permitindo o cálculo do QBER médio e do desvio padrão associado. Os resultados obtidos são apresentados na Tabela 2.

Tabela 2. Resultados experimentais do QBER para diferentes taxas de interceptação

Interceptação (%)	QBER Médio	Desvio Padrão
0	0.0000	0.0000
25	0.0477	0.0409
50	0.1302	0.0561
75	0.2084	0.0605
100	0.2490	0.0616

Observa-se um aumento progressivo do QBER à medida que a taxa de interceptação cresce. Mesmo em níveis intermediários de interceptação, já é possível identificar a presença de inconsistências na chave compartilhada entre Alice e Bob.

A Figura 3 apresenta a relação entre a taxa de interceptação e o QBER médio obtido nas simulações, permitindo uma análise visual do impacto da presença de um adversário no canal quântico.

Observa-se, a partir do gráfico, uma tendência crescente aproximadamente linear do QBER em função do aumento da taxa de interceptação. Para baixos níveis de interceptação, o QBER permanece próximo de zero, indicando baixa perturbação no sistema. À medida que a fração de qubits interceptados aumenta, verifica-se um crescimento progressivo da taxa de erro, refletindo o efeito acumulado das medições realizadas pelo adversário.

Nota-se que os valores experimentais aproximam-se do comportamento teórico esperado, especialmente em níveis mais elevados de interceptação, onde o QBER converge para

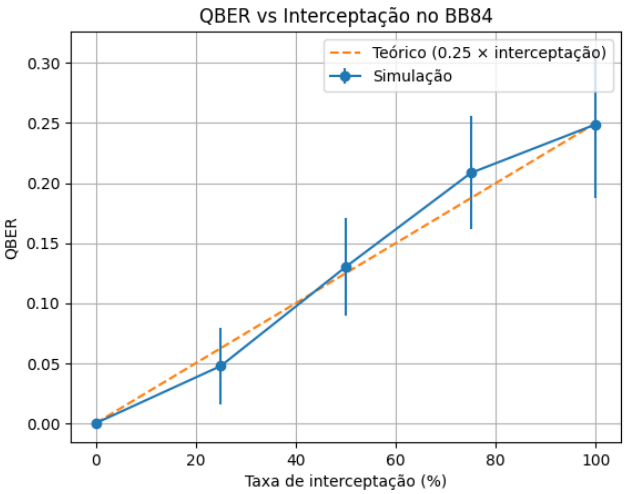

Figura 3. Relação entre taxa de interceptação e QBER no protocolo BB84

valores próximos de 25%. Esse resultado está alinhado com a análise teórica do ataque do tipo *intercept-resend*, no qual a escolha aleatória de bases pelo adversário introduz erros com probabilidade significativa.

O gráfico também evidencia a presença de variabilidade nos resultados, representada pelas barras de erro, associada à natureza probabilística das medições quânticas e ao número limitado de execuções realizadas em cada cenário. Ainda assim, a tendência geral observada permanece consistente, reforçando a validade da modelagem adotada.

A inclusão da curva teórica no gráfico permite uma comparação visual entre os valores experimentais e o comportamento esperado, evidenciando a tendência geral dos resultados obtidos.

6 Discussão

Os resultados obtidos permitem não apenas confirmar o comportamento teórico do protocolo BB84, mas também evidenciar, de forma experimental, a relação direta entre a presença de interceptação e a degradação da qualidade da chave gerada. A variação do QBER observada ao longo dos experimentos apresenta forte aderência ao comportamento esperado na literatura, reforçando a validade da modelagem adotada [Muga *et al.*, 2011; Yuen, 2012].

No cenário sem interceptação, o QBER igual a zero confirma a consistência da implementação e a ausência de erros introduzidos pelo ambiente de simulação. Esse resultado indica que, em condições ideais, o protocolo permite o estabelecimento de uma chave perfeitamente correlacionada entre as partes, desde que não haja interferência externa, comportamento alinhado com o modelo teórico do BB84, no qual erros surgem apenas na presença de ruído ou de um adversário.

A introdução do ataque do tipo *intercept-resend* permitiu observar o impacto direto da interferência no canal quântico. À medida que a taxa de interceptação aumenta, verifica-se um crescimento progressivo do QBER, evidenciando a relação entre a presença de Eve e a degradação da qualidade da chave compartilhada. Esse comportamento decorre da escolha aleatória de bases por parte do interceptador: sempre que Eve escolhe uma base incompatível com a de Alice, o estado do qubit é perturbado, introduzindo erros detectáveis após o *sifting*.

Nesse contexto, o QBER não se configura apenas como uma métrica descritiva, mas como um potencial indicador operacional de segurança, permitindo que sistemas reais orientem a aceitação ou rejeição de uma chave com base em critérios quantitativos, desde que observadas as limitações inerentes ao ambiente de simulação. Essa característica é central para a aplicação prática de protocolos de QKD, uma vez que possibilita a detecção ativa de tentativas de interceptação.

Os valores experimentais obtidos aproximam-se do limite teórico de 25% no caso de interceptação total, conforme previsto pela equação estudada e amplamente reportado na literatura [Bennett and Brassard, 2014]. Pequenas variações em relação aos valores esperados podem ser atribuídas à natureza probabilística das medições quânticas e ao número limitado de execuções realizadas por cenário. Ainda assim, a tendência observada mantém-se consistente ao longo de todos os experimentos.

Um aspecto relevante da análise refere-se ao limiar de segurança do protocolo. Na prática, valores de QBER acima de aproximadamente 11% são frequentemente considerados indicativos de comprometimento da chave, inviabilizando sua utilização [Lee *et al*., 2022]. Nos resultados obtidos, observa-se que esse limiar é ultrapassado já em níveis intermediários de interceptação, entre 50% e 75% dos qubits interceptados, sugerindo a capacidade do protocolo em detectar a presença de um adversário antes que a interceptação seja total, dentro do escopo simulado.

A variabilidade observada nos resultados, expressa pelos desvios padrão reportados na Tabela 2, reflete a natureza estocástica das medições quânticas e o impacto do número limitado de execuções por cenário. Em experimentos com maior número de amostras, espera-se uma redução dessa variabilidade, resultando em estimativas mais estáveis do QBER. Mesmo assim, os experimentos realizados foram suficientes para capturar o comportamento fundamental do sistema.

Embora os resultados estejam em conformidade com a literatura, destaca-se que o presente trabalho adota uma abordagem simplificada e reprodutível, diferindo de estudos que utilizam ambientes experimentais mais complexos ou hardware quântico real [Combarro and González-Castillo, 2025; Moizuddin *et al*., 2017]. Essa simplificação, embora limite a escala dos experimentos, permite isolar os efeitos fundamentais do protocolo e compreender de forma mais direta a relação entre interceptação e QBER.

A principal limitação da análise refere-se ao uso de um ambiente de simulação idealizado, no qual não são considerados efeitos como ruído físico, perdas no canal e imperfeições de dispositivos, fatores que impactam significativamente sistemas reais de QKD. O número reduzido de qubits e execuções, imposto por restrições computacionais, também pode influenciar a estabilidade estatística dos resultados, especialmente nos cenários intermediários de interceptação. As tendências observadas são robustas, mas os valores absolutos devem ser interpretados com cautela.

Comparando com trabalhos relacionados, os resultados obtidos estão em conformidade com análises teóricas e simulações previamente reportadas, especialmente quanto à relação aproximadamente linear entre taxa de interceptação e QBER e à convergência para o limite de 25% em interceptação total [Moizuddin *et al*., 2017; Bennett and Brassard, 2014]. A principal diferença reside na escala dos experimentos, uma vez que implementações mais avançadas frequentemente utilizam maior número de qubits e execuções.

Nesse sentido, os resultados não apenas corroboram o comportamento teórico esperado do protocolo BB84, mas ilustram, de forma acessível e reproduzível, os mecanismos fundamentais associados à sua segurança, contribuindo para a compreensão conceitual do tema e para o desenvolvimento de novas pesquisas na área.

7 Considerações Finais

Este trabalho apresentou uma análise do protocolo BB84 por meio de simulação computacional, com foco na avaliação do comportamento do QBER sob diferentes níveis de interceptação. A abordagem adotada permitiu observar, de forma clara, a relação entre a presença de um adversário no canal quântico e o aumento da taxa de erro na chave compartilhada.

Os resultados demonstraram forte aderência ao comportamento teórico esperado, especialmente no que se refere ao crescimento progressivo do QBER em função da taxa de interceptação e à aproximação do limite de 25% em cenários de interceptação total. Verificou-se ainda que níveis intermediários de interceptação já são suficientes para ultrapassar limiares teóricos de segurança esperados pelo modelo, sugerindo a capacidade do protocolo em detectar interferências no canal antes que a interceptação seja completa.

A implementação realizada, baseada em ferramentas acessíveis como Python e Qiskit, mostrou-se adequada para a análise dos princípios fundamentais do protocolo BB84 [Combarro and González-Castillo, 2025]. Os parâmetros adotados, definidos como escolha metodológica deliberada, mostraram-se suficientes para capturar as principais características do sistema e validar seu comportamento em diferentes condições experimentais. O código utilizado está disponibilizado publicamente, reforçando o compromisso com a reprodutibilidade e facilitando a extensão do trabalho por outros pesquisadores.

Do ponto de vista metodológico, destaca-se a ênfase na reprodutibilidade dos experimentos, possibilitando que o modelo desenvolvido seja facilmente replicado e adaptado para estudos futuros. Essa característica é especialmente relevante em contextos de iniciação científica, nos quais a compreensão dos fundamentos e a possibilidade de extensão do trabalho são aspectos essenciais.

Como limitações, observa-se que a análise foi conduzida em um ambiente idealizado, sem a consideração de fatores como ruído físico, perdas no canal ou imperfeições de dispositivos quânticos. Os resultados obtidos representam, portanto, uma aproximação do comportamento teórico do protocolo, não substituindo experimentos conduzidos em hardware quântico real. A inclusão desses elementos representa uma direção importante para trabalhos futuros, permitindo uma aproximação maior com cenários reais de implementação de QKD.

Futuras investigações podem explorar a comparação entre protocolos de distribuição de chaves quânticas e abordagens de criptografia pós-quântica, bem como a análise de estratégias de ataque mais sofisticadas, como ataques de fóton único ou exploração de falhas de implementação [Azevedo *et al*., 2025]. A ampliação da escala dos experimentos, com maior número de execuções e variação de parâmetros adicio-

nais, também pode contribuir para uma avaliação estatística mais robusta do comportamento do QBER.

De forma geral, os resultados obtidos em ambiente simulado sugerem a relevância do protocolo BB84 como abordagem promissora para a distribuição de chaves em um cenário de avanço da computação quântica, ilustrando sua capacidade de detectar interferências dentro do escopo teórico analisado.

Declarações complementares

Agradecimentos

Os autores agradecem ao Instituto de Tecnologia e Liderança (Inteli) pelo suporte acadêmico e infraestrutura disponibilizada para o desenvolvimento deste trabalho.

Financiamento

Este trabalho não recebeu financiamento específico de agências públicas, comerciais ou sem fins lucrativos.

Contribuições dos autores

VTH e LFP contribuíram para a concepção deste estudo. LFP realizarou os experimentos. LFP é a principal contribuidora e escritora deste manuscrito. VTH atuou na revisão do texto completo. Todos os autores leram e aprovaram o manuscrito final.

Conflitos de interesse

Os autores declaram que não possuem conflitos de interesse relacionados a este trabalho.

Disponibilidade de dados e materiais

Os códigos-fonte, scripts de simulação e instruções para reprodução dos experimentos estão disponíveis publicamente no repositório: `https://github.com/lupetenazzi/quantum-cryptography-bb84`.

Outras informações relevantes

Ferramentas de inteligência artificial generativa foram utilizadas exclusivamente para revisão de coesão textual e adaptação de imagens. O conteúdo técnico, os resultados e as interpretações científicas são de responsabilidade exclusiva dos autores.

Referências

Azevedo, C., Costa, G., and Moreira, F. (2025). Tecnologia quântica e defesa nacional oportunidades e desafios para o brasil. *Boletim de Conjuntura (BOCA)*, 23:275–299. DOI: https://doi.org/10.5281/zenodo.16384321.

Bennett, C. H. and Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7–11. DOI: 10.1016/j.tcs.2014.05.025.

Carrera-Rivera, A., Ochoa, W., Larrinaga, F., and Lasa, G. (2022). How-to conduct a systematic literature review: A quick guide for computer science research. *MethodsX*, 9:101895. DOI: https://doi.org/10.1016/j.mex.2022.101895.

Combarro, E. F. and González-Castillo, S. (2025). *A Practical Guide to Quantum Computing: Hands-on Approach to Quantum Computing with Qiskit*. Packt Publishing.

Diamanti, E. (2006). *Security and implementation of differential phase shift quantum key distribution systems*. Stanford University. Disponível em: `https://ui.adsabs.harvard.edu/abs/2006PhDT.....48D`.

Djordjevic, I. B. (2025). Quantum key distribution (qkd) fundamentals. In *Physical-Layer Security, Quantum Key Distribution, and Post-Quantum Cryptography*, pages 305–362. Springer Nature Switzerland, Cham. DOI: 10.1007/978-3-031-88372-9_7.

Forouzan, B. A. (2007). *Cryptography & network security*. McGraw-Hill, Inc.

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, STOC '96, page 212–219, New York, NY, USA. Association for Computing Machinery. DOI: 10.1145/237814.237866.

Hayashi, V. T., Ferreira, B. K., Arakaki, R., Rossetti, J. F., Terada, R., Costa, E., Filho, W., Vieira, G., Petenazzi, L., and Falcão, P. (2025). Introdução à computação quântica e impactos em criptografia. In *Simpósio Brasileiro de Cibersegurança - SBSeg*. SBC. DOI: 10.5753/sbc.17851.3.

IBM Quantum (2023). Qiskit documentation. `https://qiskit.org`. Accessed: 27 Mar. 2026.

Kejvi, K. (2023). Building a quantum key distribution system with qiskit: A hands-on guide to bb84. `https://medium.com/@kejvikejvi/building-a-quantum-key-distribution-system%2Dwith-qiskit-a-hands-on-guide-to-bb84%2D7cc49ab72baa`. Accessed: 27 Mar. 2026.

Kumar, M. and Mondal, B. (2025). A brief review on quantum key distribution protocols. *Multimedia Tools and Applications*, 84(27):33267–33306. DOI: 10.1007/s11042-024-20535-x.

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. DOI: 10.1109/TNSM.2022.3165202.

Moizuddin, M., Winston, J., and Qayyum, M. (2017). A comprehensive survey: Quantum cryptography. In *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)*, pages 98–102. DOI: 10.1109/Anti-Cybercrime.2017.7905271.

Muga, N. J., Ferreira, M. F. S., and Pinto, A. N. (2011). Qber estimation in qkd systems with polarization encoding. *Journal of Lightwave Technology*, 29(3):355–361. DOI: 10.1109/JLT.2010.2099643.

National Institute of Standards and Technology (2024). Post-quantum cryptography standardization. `https://csrc.nist.gov/projects/post-quantum-cryptography`. Accessed: 27 Mar. 2026.

Nielsen, M. A. and Chuang, I. L. (2010). *Quantum computation and quantum information*. Cambridge university press.

Pathare, A., Patil, P., Pimple, A., and Sawant, V. (2025). Experimental analysis on the bb84 quantum key distribution protocol using qiskit and ibm quantum hardware. *TechRxiv*, 2025(0212). DOI: 10.36227/techrxiv.173933577.75659816/v1.

Rusca, D., Boaron, A., Grünenfelder, F., Martin, A., and Zbinden, H. (2018). Finite-key analysis for the 1-decoy state qkd protocol. *Applied Physics Letters*, 112(17):171104. DOI: 10.1063/1.5023340.

Shor, P. (1994). Algorithms for quantum computation: dis-

crete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134. DOI: 10.1109/SFCS.1994.365700.

Silva, N. A., Ferreira, M., Mantey, S., Almeida, M., Anjos, G., Muga, N. J., and Pinto, A. N. (2025). Tecnologias quânticas em criptografia. *Gazeta de Física*, 48(1). Disponível em: `https://www.spf.pt/magazines/gfis/521`.

Stallings, W. (2006). *Cryptography and network security, 4/E*. Pearson Education India.

Yuen, H. P. (2012). Unconditional security in quantum key distribution. Disponível em: `https://arxiv.org/abs/1205.5065`.

Zhang, H., Zhu, H., He, R., *et al*. (2025). Towards global quantum key distribution. *Nature Reviews Electrical Engineering*, 2:806–818. DOI: 10.1038/s44287-025-00238-7.