Da Criptografia Clássica ao Protocolo BB84: Um Relato sobre a Revolução Quântica na Segurança da Informação

Leonardo Gonçalves - 2020228071
Gonçalo Bastos - 2020238997

Faculdade de Ciências e Tecnologia da Universidade de Coimbra

***Abstract*—Este relatório documenta o processo de análise e implementação do protocolo BB84, destacando o impacto da revolução quântica na criptografia. Inicialmente, propusemo-nos a explorar e implementar o protocolo (DV-QKD) BB84, mas aprofundámos conceitos fundamentais que moldaram a transição da criptografia clássica para a quântica, impulsionada pelo algoritmo de Shor (também implementado e testado em hardware real). Adicionalmente, discutimos os desafios práticos associados às implementações do BB84, incluindo limitações tecnológicas e soluções propostas. Explorámos ainda a evolução de protocolos baseados em variáveis discretas, como o E91 (implementado e simulado) que se baseia em entrelaçamento quântico. Por fim, abordamos brevemente a criptografia pós-quântica como uma solução alternativa para a segurança da informação, reconhecendo que está fora do escopo principal da cadeira. Este trabalho reflete, em parte, o panorama atual da criptografia e o papel central da computação quântica na sua evolução, dentro do escopo da nossa cadeira.**

I. Introdução

A segurança da informação enfrenta uma transformação histórica com o advento da computação quântica. Enquanto a criptografia clássica se baseia em problemas computacionalmente difíceis, como a fatorização de números grandes no RSA, o surgimento do algoritmo de Shor em 1994 colocou em risco a robustez desses sistemas. Este avanço, combinado com o rápido progresso no desenvolvimento de computadores quânticos, marca o início de uma segunda revolução quântica, impulsionando a busca por alternativas mais seguras.

Neste contexto, a criptografia quântica emerge como uma solução promissora, fundamentada em princípios inquebráveis da mecânica quântica, como o teorema da não-clonagem e o princípio da incerteza. O protocolo BB84, desenvolvido por Bennett e Brassard, representa o marco inicial desta área e constitui o foco central deste trabalho. Durante o desenvolvimento, expandimos o escopo para incluir outras contribuições relevantes, como o protocolo E91 e a criptografia pós-quântica, bem como os desafios práticos associados à implementação de sistemas quânticos, incluindo limitações tecnológicas e ataques de canal lateral.

Este trabalho visa explorar estas soluções, destacando o papel central da computação quântica na evolução da segurança da informação e refletindo sobre os desafios e oportunidades associados à transição para tecnologias de criptografia quântica.

II. Criptografia Clássica e o Impacto do Algoritmo de Shor

A. Criptografia Clássica

A criptografia clássica fundamenta-se em problemas computacionalmente difíceis, cuja resolução em sistemas computacionais clássicos demandaria um tempo proibitivo. Entre os algoritmos mais notáveis, destacam-se o RSA e o DES.

O RSA baseia-se na dificuldade de fatorizar números inteiros grandes. A segurança deste sistema depende de três passos principais:

1) Escolha de dois números primos grandes, p e q, cujo produto $N = p \cdot q$ é usado como base.
2) Cálculo da chave pública, e, e da chave privada, d, tais que $e \cdot d \equiv 1 \mod \phi(N)$, onde $\phi(N)$ é a função totiente de Euler.
3) Uso da chave pública para cifrar mensagens ($C = M^e \mod N$) e da chave privada para decifrá-las ($M = C^d \mod N$).

Apesar de sua robustez em cenários clássicos, o RSA é vulnerável a computadores quânticos devido à eficiência do *Algoritmo de Shor*, que resolve o problema de fatorização em tempo polinomial.

B. Impacto do Algoritmo de Shor

O *Algoritmo de Shor*, desenvolvido em 1994, revolucionou a computação ao demonstrar que problemas como a fatorização de inteiros e o cálculo de logaritmos discretos podem ser resolvidos em tempo polinomial em computadores quânticos. Este avanço é uma das principais ameaças à criptografia clássica, especialmente a sistemas como o RSA, cuja segurança depende da dificuldade de fatorização.

1) Funcionamento do Algoritmo de Shor: O algoritmo utiliza a *estimativa de fase quântica* para determinar o período de uma função periódica $f(x) = a^x \mod N$. A determinação do período permite calcular fatores de N, quebrando a base da segurança do RSA. Os passos principais do algoritmo incluem:

- Seleção de um número a, tal que $1 < a < N$, e cálculo do maior divisor comum ($\gcd$) entre a e N.

- Implementação de um circuito quântico para encontrar o período r da função $f(x)$.
- Utilização do período r para determinar fatores de N, garantindo que N seja divisível por $(a^{r/2}-1)$ ou $(a^{r/2}+1)$.

2) Insights da Implementação Qiskit: Para demonstrar o funcionamento do *Algoritmo de Shor*, foi utilizada a plataforma Qiskit para implementar o circuito quântico que realiza a estimativa de fase. O foco foi na fatorização de $N = 15$, com $a = 7$, utilizando tanto simuladores quanto hardware real.

Os principais componentes da implementação incluem:

- **Estado Inicial:** Os qubits de contagem são preparados no estado $|+\rangle$ e o registo auxiliar é inicializado no estado $|1\rangle$.
- **Operadores Controlados:** Circuitos que implementam $a^x \mod N$ de forma eficiente.
- **QFT Inversa:** Utilizada para extrair a fase correspondente ao período da função.

3) Testes e Resultados com Simulador: Os testes do *Algoritmo de Shor* foram realizados em um simulador quântico 'Aer_Simulator' usando Qiskit, focados na fatorização de $N = 15$ com $a = 7$. A execução do circuito resultou nas medições representadas no histograma da Figura 1, com análises detalhadas a seguir.

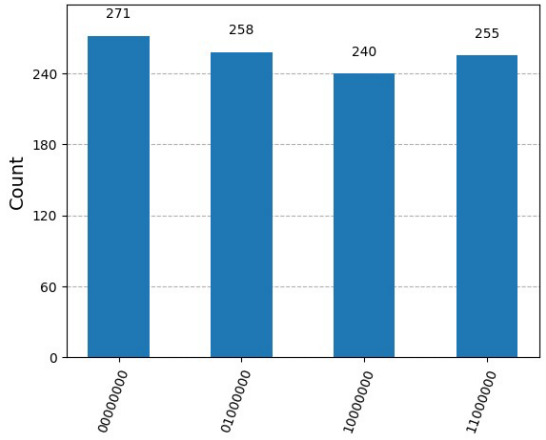

Fig. 1. Histograma das medições do *Algoritmo de Shor* no simulador para $N = 15$ e $a = 7$.

Análise dos Resultados- O histograma mostra as frequências(contagens) dos valores medidos no registo quântico após simular o circuito. Com 8 qubits alocados para o registo de medição, os valores binários medidos correspondem às seguintes fases:

$$\text{Fases Medidas: } \frac{0}{256}, \frac{64}{256}, \frac{128}{256}, \frac{192}{256}$$

Estas fases foram convertidas para números decimais e analisadas usando o algoritmo de frações contínuas para determinar o período r da função $f(x) = a^x \mod N$. A Tabela I apresenta os resultados detalhados.

Register Output (bin)	Decimal Value	Phase	Guess for r
00000000	0	0/1	-
01000000	64	1/4	4
10000000	128	1/2	4
11000000	192	3/4	4

TABLE I
FASES MEDIDAS E VALORES ASSOCIADOS AO PERÍODO r NO SIMULADOR.

Determinar o Período r Entre os valores medidos, dois resultados distintos, $1/4$ e $3/4$, levaram à determinação correta do período $r = 4$, como esperado para $N = 15$ com $a = 7$. Isso permitiu calcular os fatores de N como 3 e 5 usando a relação:

$$\text{Fatores: } (a^{r/2}-1) \mod N \quad \text{e} \quad (a^{r/2}+1) \mod N$$

Considerações Adicionais - Em algumas execuções, o valor de fase 0 foi medido. Esse resultado corresponde a um caso de $s = 0$, que não contribui para a determinação de r. Esse problema pode ser resolvido repetindo o algoritmo para obter novos resultados válidos. - A precisão do simulador permitiu identificar padrões claros no histograma, demonstrando a funcionalidade do circuito implementado.

Os resultados obtidos confirmam o comportamento esperado do *Algoritmo de Shor* em ambiente simulado, destacando sua eficácia para resolver problemas de fatorização em casos controlados.

4) Testes e Resultados em Hardware Real: Com o objetivo de explorar os desafios práticos na implementação do *Algoritmo de Shor* em hardware quântico, realizámos uma execução experimental para o caso de $N = 15$. Esta implementação foi realizada no backend `ibm_kyiv` da IBM, utilizando circuitos otimizados para o número limitado de qubits disponíveis e explorando resultados obtidos em configurações distintas. Reconhecemos, no entanto, as limitações tecnológicas do hardware atual, incluindo ruído, decoerência e fidelidade limitada das portas quânticas. Os testes foram realizados para 2048 shots e demoraram aproximadamente 1 min.

O histograma de uma das medições está apresentado na Figura 2.

É importante notar que os valores com maior número de contagens correspondem a guesses de $r = 15$, que, embora satisfaçam $r \cdot 1 = 15$, não são válidos neste contexto, uma vez que $r = N$ não é um período significativo para o algoritmo.

Análise dos Resultados- Os resultados obtidos em hardware real apresentam várias considerações importantes relacionadas com a implementação do *Algoritmo de Shor* no backend `ibm_kyiv`. Após processar os registos de saída dos circuitos quânticos, as fases medidas foram convertidas para frações aproximadas e, posteriormente, utilizadas para estimar valores candidatos para o período r. A análise indicou que, embora o algoritmo tenha conseguido gerar algumas guesses corretas para r, também foram observadas diversas medições incorretas, refletindo os desafios práticos impostos pelas limitações do hardware quântico atual.

Dos 2048 *shots* realizados, os dados mostram uma proporção significativa de guesses inválidas, com uma taxa de

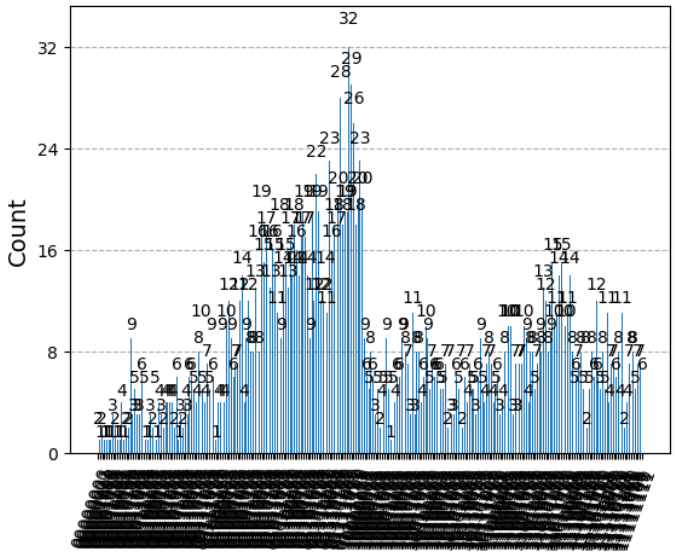

Fig. 2. Histograma resultados da execução inicial em hardware real com 1024 *shots*.

erro calculada de aproximadamente 80%. Este valor elevado deve-se, principalmente, aos seguintes fatores:

- **Ruído quântico**: O backend `ibm_kyiv` apresenta limitações na fidelidade das operações quânticas, resultando em medições desviadas da expectativa teórica.
- **Decoerência**: Durante a execução dos circuitos, os estados quânticos tendem a perder coerência devido à interação com o ambiente, comprometendo a precisão dos resultados.
- **Tamanho limitado dos circuitos**: Para circuitos mais complexos, as probabilidades de erro aumentam, tornando a identificação de r mais difícil.

A Tabela II mostra alguns resultados obtidos para as fases medidas e as guesses correspondentes para r e resultados obtidos na Figura 3, incluindo a verificação de validade de cada guess:

TABLE II
ANÁLISE DAS FASES MEDIDAS E GUESSES PARA r.

Phase (fase)	Fraction (fração)	Guess for r	Is Valid
0.320312	4/13	13	Não
0.226562	3/13	13	Não
0.593750	3/5	5	Sim
0.453125	5/11	11	Não
0.417969	5/12	12	Não
...	...	...	...

```
[246 rows x 4 columns]
Número de guesses válidas: 34
Número de guesses inválidas: 212
Taxa de erro: 86.18%
```

Fig. 3. Resultados finais da execução Algo.Shor em hardware real com 1024 *shots*.

Apesar das dificuldades, os resultados demonstram a capacidade do algoritmo em identificar valores candidatos para r, mesmo em condições adversas. A presença de guesses corretas valida a aplicação teórica do algoritmo e mostra o progresso na implementação prática do *Algoritmo de Shor* em hardware quântico.

Com base nestes resultados, futuras implementações podem beneficiar de técnicas avançadas de mitigação de erros, circuitos mais robustos e a utilização de hardware com maior número de qubits e melhor fidelidade. Estas melhorias serão essenciais para reduzir a taxa de erro e aumentar a precisão das medições, aproximando os resultados práticos dos valores teóricos esperados.

5) Limitações: Embora o algoritmo tenha se mostrado eficiente para $N = 15$, sua aplicação prática para números maiores enfrenta desafios, incluindo:

- Necessidade de hardware com qubits físicos de alta fidelidade para implementar sistemas maiores.
- Limitações impostas pela decoerência e pelo ruído em hardware atual.

6) Conclusão: O *Algoritmo de Shor* representa um marco na computação quântica, demonstrando seu impacto potencial na segurança da informação. Até agora, a execução bem-sucedida do algoritmo de Shor em computadores quânticos foi apenas para fins de demonstração e não para números grandes, como aqueles usados em criptografia RSA (números com 2048 ou mais bits). A capacidade de fatorizar números maiores será possível com o avanço da computação quântica e a construção de computadores quânticos de grande escala com milhões de qubits e baixa taxa de erro. A primeira solução proposta para este problema está apresentada a seguir.

III. CRIPTOGRAFIA QUÂNTICA

A criptografia quântica é uma área interdisciplinar da ciência da computação e da física que utiliza princípios da mecânica quântica para criar sistemas de comunicação seguros. A sua principal aplicação é a *Quantum Key Distribution* (QKD), que permite a partilha de chaves secretas entre duas partes de forma segura, mesmo na presença de um atacante.

Neste trabalho, focamo-nos na implementação e análise de dois protocolos de QKD baseados em *variáveis discretas* (DV-QKD). Estes protocolos, que dependem de medições de estados discretos, destacam-se por serem os mais estudados e implementáveis em hardware real. O primeiro é o protocolo *prepare-and-measure* BB84, e o segundo é o protocolo E91, que utiliza o entrelaçamento quântico como recurso para garantir segurança. A escolha destes protocolos permite explorar diferentes abordagens dentro do contexto da QKD.

A. Protocolo BB84

O protocolo BB84, desenvolvido por Bennett e Brassard em 1984, é um protocolo de *prepare-and-measure*, onde qubits são preparados em diferentes estados quânticos e enviados para o recetor. A segurança do protocolo baseia-se no princípio da incerteza da mecânica quântica e no teorema da não-clonagem. As etapas deste protocolo baseiam-se em:

Gerar bits e bases aleatórias por Alice.
Codificação dos bits em qubits.
Envio dos qubits para Bob através de um canal quântico (Simulado ou usando Registos Quânticos e Clássicos).
Medição dos qubits por Bob usando bases aleatórias (medição usando simulador ou HW real).
Comparação de bases para formar uma chave partilhada.

1) Implementação do BB84: Para implementar o protocolo BB84, utilizámos a biblioteca Qiskit juntamente com a biblioteca `random` do Python. O protocolo foi implementado para simulação em ambientes ideais e cenários com interceção, bem como para execução em hardware real na plataforma IBM Quantum. Além disso, foi criado um circuito quântico para gerar números aleatórios, representando os bitstrings de Alice. Este circuito tira proveito das propriedades da mecânica quântica, como a superposição, para garantir uma geração verdadeiramente aleatória de bits.

A implementação seguiu as etapas clássicas do BB84:

- **Geração de Bits e Bases Aleatórios:** Alice gerou uma sequência de bits e bases (Z e X) aleatórios, simulando a preparação dos estados quânticos.
- **Codificação:** Os bits de Alice foram codificados em qubits utilizando portas X e Hadamard (H), dependendo da base escolhida.
- **Envio dos Qubits:** Os qubits foram enviados para Bob através de um canal quântico ideal (simulado sem ruído) ou para hardware real.
- **Medição por Bob:** Bob utilizou bases aleatórias para medir os qubits recebidos. Para medições na base X, aplicou uma porta Hadamard antes da medição.
- **Comparação de Bases:** Alice e Bob comunicaram através de um canal clássico para identificar as bases em comum e descartar as que não coincidiram.

a) Simulação em Ambiente Ideal: No ambiente ideal, o canal quântico simulado não introduziu ruído ou perdas, permitindo explorar o comportamento teórico do protocolo:

- Após a comparação entre as bases de Alice e Bob, foi gerada uma chave com comprimento final de 141 bits, após o descarte dos primeiros 100 bits para evitar possíveis ataques.
- A correspondência entre as chaves de Alice e Bob foi praticamente perfeita, com uma taxa de sucesso de 100%.
- O comprimento da chave final variou conforme o número de bases em comum, que depende da probabilidade de 50% de coincidência em cada base.

b) Simulação de Interceção por Eve: Simulámos a interceção de Eve no canal quântico:

- Eve escolheu bases aleatórias para medir os qubits enviados por Alice e os retransmitiu para Bob.
- A presença de Eve introduziu "ruído" no sistema, alterando os estados quânticos dos qubits e denunciando imediatamente a interceção.
- A taxa de sucesso foi reduzida para aproximadamente 85%, evidenciando as medições incorretas resultantes da interferência de Eve.

c) Testes em Hardware Real: Para realizar medições no hardware real (`ibm_quito`), foi desenvolvida a função `measure_on_Real_HW`, que:

- Configura os qubits recebidos e aplica as medições nas bases Z e X.
- Utiliza o backend real para executar os circuitos e obter os resultados das medições.

Os testes realizados no backend real apresentaram:

- Taxa de correspondência de aproximadamente 80%, devido à decoerência e ao ruído no hardware.
- Limitações práticas relacionadas à fidelidade das operações quânticas e ao tempo de vida dos qubits no sistema.

2) Resultados e Discussão:

a) Ambiente Ideal (Sem Ruído e Sem Interceção): No ambiente ideal, o protocolo alcançou uma taxa de eficiência de 96.40%. Este resultado reflete a correspondência quase perfeita entre os bits gerados por Alice e Bob, devido à ausência de interferências externas. A chave final gerada tinha um comprimento consistente com as bases compartilhadas aleatoriamente.

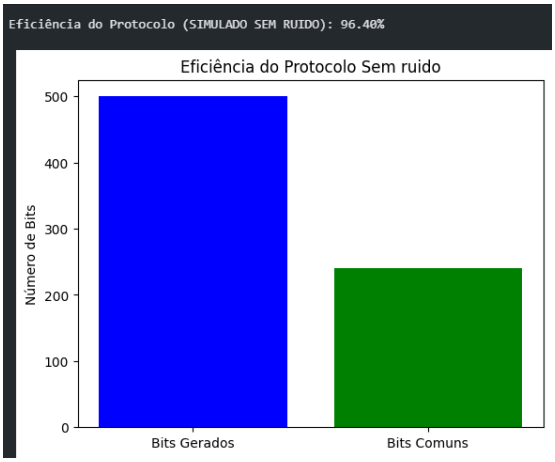

Fig. 4. Eficiência do Protocolo em Ambiente Ideal (Simulado Sem Ruído).

b) Simulação com Interceção por Eve: Ao simular a interceção de Eve, a eficiência do protocolo foi reduzida para 80.40%. Este resultado demonstra o impacto da interceção no canal quântico, onde os estados quânticos medidos por Eve introduziram "ruído" e alteraram os resultados de medição de Bob. A discrepância nos bits compartilhados denunciou a presença de Eve.

c) Testes em Hardware Real (Sem Interceção): Os testes realizados no backend `ibm_quito` evidenciaram o impacto do ruído do hardware real. Apesar disso, o protocolo alcançou uma eficiência de 96.40%, semelhante à do ambiente ideal. Estes resultados foram limitados pela decoerência e pela fidelidade das operações quânticas.

d) Testes em Hardware Real com Interceção por Eve: Quando combinados os efeitos do ruído do hardware real com a interceção por Eve, a eficiência do protocolo foi reduzida para 76.80%. Este resultado reflete a acumulação dos impactos

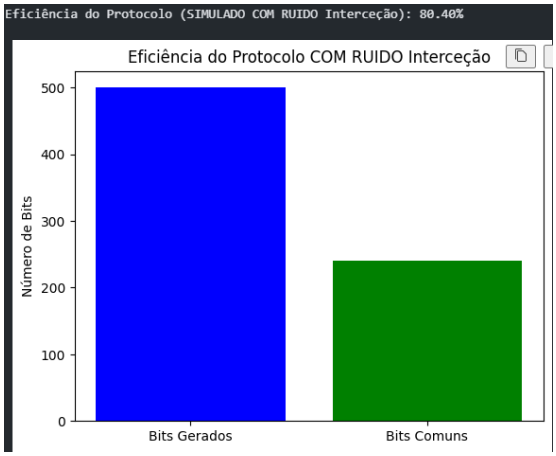

Fig. 5. Eficiência do Protocolo com Ruído Introduzido pela Interceção (Simulado).

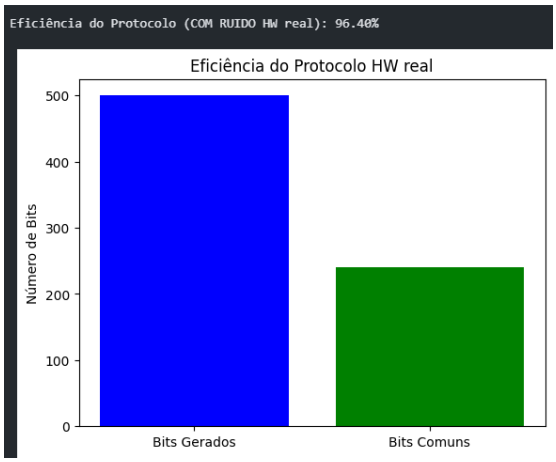

Fig. 6. Eficiência do Protocolo em Hardware Real (Com Ruído, Sem Interceção).

do ruído quântico no hardware e da interferência externa simulada.

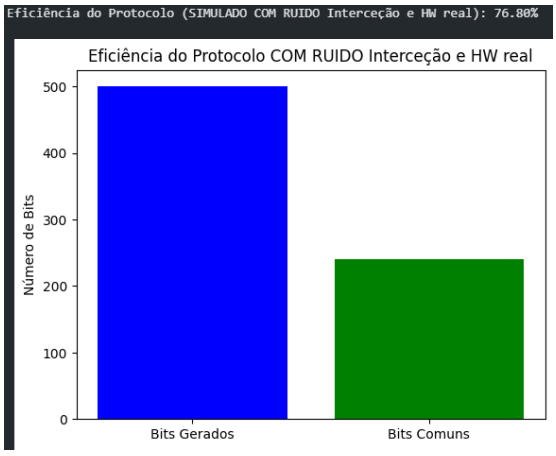

Fig. 7. Eficiência do Protocolo com Ruído do Hardware Real e Interceção.

3) Conclusão: A implementação do protocolo BB84 demonstrou ser eficaz em ambientes ideais, com resultados consistentes e correspondência perfeita entre as chaves de Alice e Bob. Contudo, as simulações de interceção e os testes em hardware real evidenciaram desafios práticos, como a introdução de ruído e a decoerência dos qubits. É importante notar que o ruído das medições em hardware real não introduz erros significativos, sendo que o impacto na eficiência do protocolo está principalmente associado aos erros introduzidos pelo canal de comunicação. No entanto, a presença de interceções impactou significativamente a taxa de sucesso. Estes resultados reforçam a necessidade de avanços tecnológicos no hardware quântico e nos canais de comunicação para viabilizar implementações mais robustas e seguras em sistemas reais.

B. Protocolo E91

1) Descrição do Algoritmo: O protocolo E91 baseia-se no entrelaçamento quântico para permitir a distribuição de chaves seguras entre dois participantes, Alice e Bob. Charlie prepara pares de qubits no estado singlet $|\psi_s\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ e distribui os qubits entre Alice e Bob. Em seguida, os participantes realizam medições nas suas qubits em direções aleatórias escolhidas a partir de um conjunto pré-definido. As correlações resultantes são analisadas através do cálculo do valor CHSH para verificar a presença de entrelaçamento. Se a desigualdade de Bell for violada ($CHSH > 2$), a chave gerada é considerada segura.

2) Simulação Sem Interferência: Na simulação sem interferência, os pares entrelaçados são gerados e distribuídos entre Alice e Bob. As medições são realizadas em diferentes bases (X, Z, W, V), e os resultados são usados para calcular as chaves k e k' de Alice e Bob. Para avaliar a presença de entrelaçamento, o valor CHSH é calculado a partir das correlações. No entanto, no hardware real utilizado, o valor CHSH obtido foi 0.1094, muito abaixo do limiar de 2, indicando a ausência de entrelaçamento devido ao ruído e limitações do hardware.

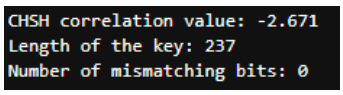

Fig. 8. Resultados CHSH da simulação sem Interferência

3) Cálculo de Correlação: O cálculo de correlação entre os resultados de Alice e Bob baseia-se nas probabilidades de diferentes combinações de medições. A correlação para uma base $A \otimes B$ é dada por:

$$\langle A \otimes B \rangle = P(00) + P(11) - P(01) - P(10),$$

onde $P(ab)$ representa a probabilidade de Alice e Bob obterem os resultados a e b, respetivamente. Estas correlações são combinadas para calcular o valor CHSH:

$$CHSH = |E(a_0, b_0) - E(a_0, b_1) + E(a_1, b_0) + E(a_1, b_1)|,$$

onde $E(a_i, b_j)$ são as correlações calculadas para diferentes combinações de bases.

4) Simulação com Interferência: Na simulação com interferência, Eve utiliza a técnica de *intercept-resend*, onde intercepta os qubits de Alice e Bob, mede as projeções de spin, e envia novos qubits preparados com base nos resultados obtidos ($|01\rangle$ ou $|10\rangle$). Esta interferência provoca desvios significativos no valor CHSH e introduz discrepâncias nas chaves de Alice e Bob. O número de erros aumenta proporcionalmente à interferência de Eve, comprometendo a segurança da comunicação. Na simulação, os resultados demonstraram que o valor CHSH está longe do esperado $-2\sqrt{2}$, confirmando a presença de interferência e a incapacidade de usar as chaves geradas.

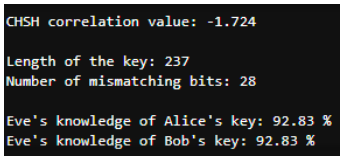

Fig. 9. Resultados Simulação com Evesdroping

a) Testes em Hardware Real: Os resultados obtidos na simulação em hardware quântico real, com um valor CHSH de 0.1094 e uma elevada taxa de discrepância entre as chaves de Alice e Bob (113,616 de 114,688 bits), refletem as limitações atuais dos dispositivos quânticos. A presença de ruído elevado, erros nas operações quânticas (como portas CNOT e medições) e a decoerência dos estados quânticos levam à degradação do entrelaçamento e à ausência de correlações mensuráveis. Além disso, a falta de mecanismos de correção de erros e tolerância a falhas em dispositivos quânticos atuais contribui para a aleatoriedade nos resultados e impede a preservação do entrelaçamento. Estes resultados são esperados no estado atual da tecnologia quântica e podem ser melhorados no futuro com avanços em hardware e técnicas de mitigação de erros.

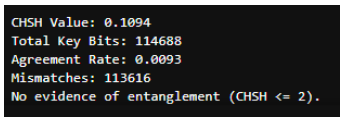

Fig. 10. Resultados Simulação HW real

5) Resultados e Discussão:

- **Simulação em Ambiente Ideal:** Correlações perfeitas entre Alice e Bob, validando o protocolo.
- **Hardware Real:** A execução apresentou correlações muito baixas, o que mostrou a falta de entrelaçamento entre os estados devido a limitações do hardware.

6) Limitações do E91: O protocolo E91 enfrenta desafios adicionais em comparação ao BB84:

- A necessidade de gerar e manter pares entrelaçados em grandes distâncias.
- Sensibilidade extrema ao ruído e à decoerência.
- Requisitos computacionais mais elevados para verificar desigualdades de Bell.

7) Conclusão do E91: No futuro, espera-se que avanços em hardware quântico, como dispositivos com menor ruído, maior fidelidade nas operações e implementação de correção de erros quânticos, permitam a execução confiável do protocolo E91 em cenários práticos. Além disso, a integração de técnicas de mitigação de erros pode melhorar a preservação do entrelaçamento e a correlação nas medições. O protocolo E91 apresenta vantagens em relação ao BB84 por basear-se diretamente no entrelaçamento quântico, garantindo segurança fundamentada na violação da desigualdade de Bell, o que o torna mais robusto contra ataques sofisticados e permite a verificação explícita da presença de entrelaçamento durante a comunicação.

C. Comparação entre BB84 e E91

A Tabela III apresenta uma comparação entre os dois protocolos implementados.

TABLE III
COMPARAÇÃO ENTRE OS PROTOCOLOS BB84 E E91.

Característica	**BB84**	**E91**
Base Teórica	Prepare-and-measure	Entrelaçamento quântico
Requisitos Tecnológicos	Moderados	Elevados
Robustez ao Ruído	Baixa	Moderada
Eficiência Prática	Elevada	Moderada

D. Conclusão Geral

Os protocolos BB84 e E91 representam abordagens distintas para a QKD, cada um com vantagens e limitações específicas. Enquanto o BB84 é mais viável para implementações práticas em hardware atual, o E91 apresenta maior robustez teórica, mas requer avanços tecnológicos para alcançar uma aplicação eficiente.

IV. CRIPTOGRAFIA PÓS-QUÂNTICA

A criptografia pós-quântica surge como uma alternativa clássica e complementar à criptografia quântica, visando proteger sistemas de informação contra ataques realizados por computadores quânticos. Estas soluções, ao contrário da QKD, são implementadas em algoritmos clássicos que não dependem de hardware quântico, mas oferecem segurança baseada em problemas matemáticos que atualmente não possuem algoritmos eficientes conhecidos, nem clássicos nem quânticos.

As principais abordagens incluem:

- **Lattice-based cryptography:** Utiliza problemas baseados em redes euclidianas (lattices), como a dificuldade em encontrar o vetor mais curto em uma rede, para garantir segurança.
- **Code-based cryptography:** Baseia-se em problemas de decodificação de códigos de correção de erros, como os códigos de McEliece.
- **Hash-based signatures:** Utiliza funções hash para criar assinaturas digitais seguras.
- **Multivariate quadratic equations:** Baseia-se na dificuldade de resolver sistemas de equações quadráticas multivariáveis.

Embora estas técnicas sejam promissoras e estejam a ser padronizadas por iniciativas como o NIST (National Institute

of Standards and Technology), elas apresentam desafios, como chaves de tamanho elevado e desempenho inferior em comparação com os algoritmos clássicos amplamente utilizados, como RSA e AES.

Complementaridade com a QKD A criptografia pós-quântica é frequentemente vista como uma solução complementar à QKD. Enquanto a QKD oferece segurança baseada em princípios fundamentais da mecânica quântica, a criptografia pós-quântica fornece alternativas práticas que não dependem de infraestruturas quânticas. Uma abordagem híbrida, combinando ambas as tecnologias, pode maximizar a segurança, integrando a robustez teórica da QKD com a flexibilidade das soluções pós-quânticas em redes clássicas.

V. Estado da Arte e Perspectivas Futuras

A. Avanços em QKD

A criptografia quântica, uma área emergente que combina física quântica e ciência da computação, está a revolucionar a segurança das comunicações ao oferecer métodos fundamentados nas leis fundamentais da mecânica quântica. Protocolos como o BB84, que utiliza propriedades de superposição de estados quânticos, e o E91, que explora o entrelaçamento quântico e as desigualdades de Bell, estabeleceram as bases para a distribuição de chaves quânticas (QKD). O protocolo E91, em particular, destaca-se pela capacidade de verificar a presença de entrelaçamento, garantindo segurança inerente contra interferências externas.

Testes recentes têm demonstrado a viabilidade prática da QKD. O satélite chinês Micius, por exemplo, conseguiu distribuir chaves quânticas entre continentes, como na comunicação entre a China e a Áustria, alcançando uma distância de aproximadamente 7.600 km. Além disso, redes terrestres de QKD têm sido implementadas, como a rede quântica em Hefei, na China, que conecta múltiplos nós com alta eficiência. Estes avanços evidenciam o progresso no uso de QKD em cenários reais.

Os avanços teóricos e experimentais mais recentes incluem:

- **Protocolos Device-Independent (DI-QKD):** Garantem segurança mesmo na presença de dispositivos quânticos comprometidos, eliminando a necessidade de confiar nos dispositivos utilizados. Apesar das vantagens, ainda apresentam desafios como baixas taxas de chave e altos requisitos tecnológicos.
- **Continuous-Variable QKD (CV-QKD):** Utilizam estados gaussianos contínuos em vez de variáveis discretas, possibilitando maior integração com a infraestrutura de fibra ótica existente.
- **Redes e Repetidores Quânticos:** Avanços em repetidores quânticos permitem superar as limitações de perda de sinal em canais quânticos ponto-a-ponto, expandindo a QKD para redes globais.

Adicionalmente, experiências como as realizadas pelo Instituto Nacional de Padrões e Tecnologia (NIST) nos EUA têm explorado a implementação de QKD combinada com criptografia pós-quântica em redes comerciais, destacando a aplicabilidade híbrida.

B. Criptografia Híbrida

A integração de QKD com algoritmos de criptografia pós-quântica é uma solução promissora para sistemas críticos. Estas soluções híbridas combinam a segurança teórica da QKD com a eficiência prática de algoritmos resistentes à computação quântica. Exemplos incluem:

- Sistemas de redundância mútua: Combina QKD e algoritmos pós-quânticos para garantir segurança mesmo se uma das abordagens for comprometida.
- Integração em redes definidas por software (SDN): Permitem a adaptação dinâmica entre diferentes métodos de criptografia com base no nível de ameaça.

C. Desafios e Oportunidades

Apesar dos avanços, a implementação prática de QKD enfrenta desafios significativos:

- **Decoerência e Ruído:** A interação dos qubits com o ambiente externo degrada o emaranhamento e reduz a fidelidade das medições.
- **Escalabilidade:** Redes quânticas globais requerem avanços em repetidores quânticos e fontes de fotões únicos.
- **Custo e Infraestrutura:** A QKD ainda é cara e complexa, o que dificulta a sua adoção em ambientes comerciais.
- **Padronização:** A interoperabilidade e a adoção em larga escala exigem esforços globais de padronização.

D. Perspectivas Futuras

No futuro, espera-se que a criptografia quântica atinja níveis de robustez e escalabilidade suficientes para aplicações práticas em redes globais. Os avanços mais promissores incluem:

- **Repetidores Quânticos Avançados:** Capazes de preservar o entrelaçamento em longas distâncias, permitindo a criação de redes quânticas de alta fidelidade.
- **Satélites para QKD:** Como o Micius, aumentando a conectividade global com comunicações ultra-seguras entre continentes.
- **Protocolos de Correção de Erros:** Reduzindo o impacto do ruído e da decoerência em operações quânticas.
- **Integração de Tecnologias Quânticas Híbridas:** Combinação de arquiteturas baseadas em iões aprisionados e supercondutores para maior eficiência e menor impacto de erros.

Com a crescente capacidade tecnológica, espera-se que experiências como a de Hefei e o uso de satélites inspirem uma Internet Quântica global, permitindo comunicações ultra-seguras e novas formas de processamento de informação, essenciais para proteger dados sensíveis em uma era onde a computação quântica se torna uma realidade prática.

VI. Conclusão

O trabalho revelou a amplitude da revolução quântica na criptografia, desde o impacto disruptivo do algoritmo de Shor até as inovações práticas no BB84 e E91. A implementação

em hardware real evidenciou desafios tecnológicos, como a gestão de ruído e perdas. Futuras investigações podem explorar melhorias em correções de erros e a integração de hardware otimizado para sistemas QKD.

VII. References

[1] C. H. Bennett and G. Brassard, *"Quantum Cryptography: Public Key Distribution and Coin Tossing"*, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 1984.

[2] S. Pirandola, *"Advances in quantum cryptography"*, Advances in Optics and Photonics, DOI: 10.1364/AOP.361502.

[3] P. W. Shor, *"Algorithms for quantum computation: discrete logarithms and factoring"*, Proceedings 35th Annual Symposium on Foundations of Computer Science, 1994.

[4] Wikipedia, *"NIST Post-Quantum Cryptography Standardization"*, disponível em: https://en.wikipedia.org/wiki/NIST_Post-Quantum_Cryptography_Standardization, acesso em Janeiro de 2025.

[5] Wikipedia, *"Harvest now, decrypt later"*, disponível em: https://en.wikipedia.org/wiki/Harvest_now,_decrypt_later, acesso em Janeiro de 2025.

[6] Qiskit Textbook, *"Quantum Key Distribution Notebook"*, disponível em: https://github.com/Qiskit/textbook/blob/main/notebooks/ch-algorithms/quantum-key-distribution.ipynb, acesso em Janeiro de 2025.

[7] Qiskit Community, "E91 Quantum Key Distribution Protocol," *Qiskit Community Tutorials*, 2018, [Online]. Available: https://github.com/qiskit-community/qiskit-community-tutorials/blob/master/awards/teach_me_qiskit_2018/e91_qkd/e91_quantum_key_distribution_protocol.ipynb.