CRIPTOANALISTAS 5.0 O PODER DA IA NA DECODIFICAÇÃO DE DADOS

"EXPLORA COMO A INTELIGÊNCIA ARTIFICIAL E A COMPUTAÇÃO HÍBRIDA COMBINANDO TÉCNICAS CLÁSSICAS E QUÂNTICAS ESTÃO TRANSFORMANDO A SEGURANÇA DE DADOS"

INTRODUÇÃO

Em um cenário onde os avanços da computação quântica ameaçam a criptografia tradicional, desenvolvemos uma abordagem híbrida que utiliza algoritmos clássicos, como o AES, e algoritmos pós-quânticos, como o Grover, para garantir a proteção dos dados.

Além disso, o uso do algoritmo de Grover permite acelerar a busca por chaves, aumentando a segurança e eficiência.

Essa pesquisa aponta o caminho para um futuro onde sistemas de criptografia estarão prontos para lidar com as ameaças emergentes de um mundo digital cada vez mais avançado.

OBJETIVO(S) DA PESQUISA

Explorar o impacto da IA e da computação híbrida na criptoanálise moderna.

- Segurança híbrida (clássico + quântico)

- Papel da IA na identificação de vulnerabilidades

PERCURSO METODOLÓGICO

Integração de criptografia clássica (AES) e algoritmos quânticos
de próxima geração.

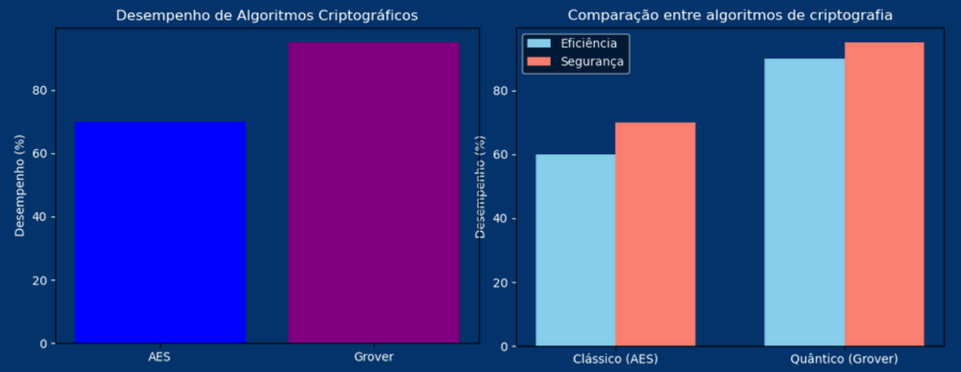
Aplicação do Algoritmo de Grover para otimizar a busca de chaves em redes neurais profunda.

ANÁLISE E/OU RESULTADOS

Comparação de desempenho entre algoritmos

- AES vs. Grover

- Algoritmo Grover para busca otimizada



PESQUISADOR(A) PRINCIPAL

Autor: Andson Andre Ribeiro
Título: Criptoanalistas 5.0 O Poder da IA na Decodificação de Dados
Contato: ra00306954@pucsp.edu.br
Pontifícia Universidade Católica de São Paulo

CONCLUSÕES Principais Descobertas e Valor do Estudo

- Eficiência da IA na Criptoanálise: A pesquisa destaca como a inteligência artificial, integrada a métodos quânticos, pode aumentar a eficiência da decodificação de dados, aprimorando a segurança de sistemas críticos.
- Resiliência com Algoritmos Pós-Quânticos: A aplicação de algoritmos como o Kyber e o Grover mostra-se promissora para resistir a ataques de computadores quânticos, uma preocupação crescente na segurança cibernética.

COLABORADORES

Professor Orientador: David de Oliveira Lemes
Pontifícia Universidade Católica de São Paulo

PRINCIPAL REFERENCIAL TEÓRICO

1. GROVER, LK Um algoritmo mecânico quântico rápido para pesquisa de banco de dados. In: Anais do vigésimo oitavo simpósio anual da ACM sobre Teoria da Computação, STOC '96. Nova York, NY, EUA: Association for Computing Machinery, jul. 1996, pág. fachada:10.1145/237814.237866. Disponível em: Acesso em: 23 jun. 2024

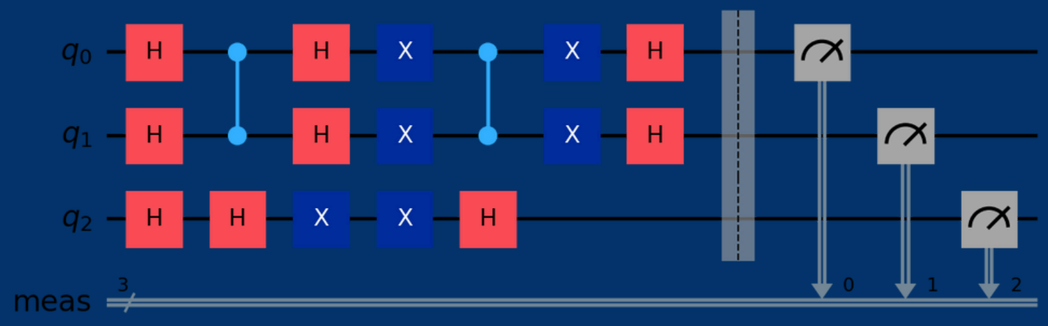
CRIPTOANALISTAS 5.0 O PODER DA IA NA DECODIFICAÇÃO DE DADOS

“EXPLORA COMO A INTELIGÊNCIA ARTIFICIAL E A COMPUTAÇÃO HÍBRIDA COMBINANDO TÉCNICAS CLÁSSICAS E QUÂNTICAS ESTÃO TRANSFORMANDO A SEGURANÇA DE DADOS”

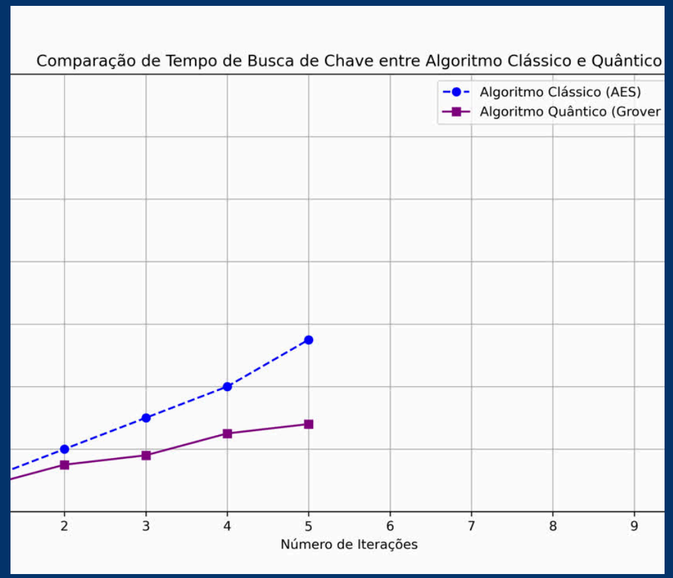
5º CONGRESSO DE INTELIGÊNCIA ARTIFICIAL 2024 PUC-SP

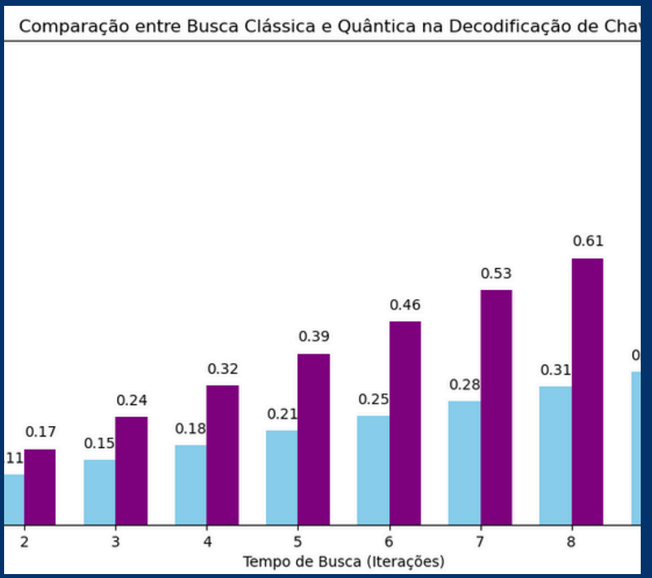
LAYOUT: CIRCUITO QUÂNTICO QISKIT EM PYTHON

```
oracle = Diagonal([1] * 7 + [-1])
qc = QuantumCircuit(3)
qc.h([0, 1, 2])
qc =
qc.compose(GroverOperator(oracle))
qc.draw(output="mpl", style="iqp")
```



Descobertas e Valor do Estudo





CONCLUSÕES (CONT.)

Limitações

- **Acesso limitado a Computação Quântica: A pesquisa depende de recursos ainda em desenvolvimento, como computação quântica plena, o que limita testes e resultados em grande escala.**

Contribuição e Impacto Futuro.

- **Avanços na Segurança de Dados: A abordagem híbrida serve como modelo para novas soluções de segurança adaptáveis a ameaças futuras, especialmente com o avanço da computação quântica.**
- **Aplicações Práticas: Este estudo pode ser aplicado para proteger dados em áreas sensíveis, como finanças e defesa, estabelecendo uma base para futuras pesquisas e desenvolvimento em criptografia híbrida.**

Chave Pública	Probabilidade Clássica (AES)	Probabilidade Quântica (Grover)
)y1Q:ihd-'Xh0'Rln1	0.08	0.1
Xgsb_J?9"UV[1D	0.11333333333333334	0.17222222222222222
p>^/%d#Z%hg#x4^	0.14666666666666667	0.24444444444444446
8J9>n%M}$l	0.18	0.31666666666666665
PD'N>#l@Q1T3SY7RX.	0.21333333333333332	0.38888888888888895
nCL?c-a<o>``){,tZtW	0.24666666666666665	0.46111111111111114
>Ov+knn9.DT^%N,0	0.28	0.5333333333333333
pOHZ7x0O(pw{F+WY	0.31333333333333335	0.6055555555555556
>Wmmr"#n,y	0.3466666666666667	0.6777777777777778
a1b2c3d4e5	0.38	0.75

Resultado da Decodificação

have Decodificada: a1b2c3d4e
Chave Privada: 0a1b2c3d4e

PUC-SP FCET tidd PUC CAMPINAS