Criptoanalistas 5.0 O Poder da IA na Decodificação de Dados

Cryptonanalyst 5.0 The Power Of AI In Data Decoding

Autor - Andson Andre da Silva Ribeiro
andreandson09@gmail.com
Ciências de Dados e Inteligência Artificial
Professor Orientador - David de Oliveira Lemes

Resumo

Este artigo examina os avanços, desafios da computação híbrida na quinta geração de tecnologia, destacando o papel importante da inteligência artificial (IA) neste campo. A computação híbrida combina diferentes paradigmas computacionais melhorar o desempenho e resolver problemas complexos. A IA, com seus algoritmos sofisticados aprendizado de máquina aprimora a capacidade processamento e introduz adaptabilidade, tornando a computação autônoma e eficiente. Este estudo também discute as implicações práticas desses avanços para a segurança dados e sugere direções para futuras pesquisas.

Palavras-chave: Ciências Dados. Inteligência Artificial. Aprendizado Máquina. Computação Clássica. Computação Quântica. Algoritmo Otimização.

Abstratc

This article examines the advances and challenges of hybrid computing in the fifth generation of technology, highlighting the important role of artificial intelligence (AI) in this field. Hybrid computing combines different computing paradigms to improve performance and solve complex problems. AI, with its sophisticated algorithms and machine learning, enhances processing power and introduces adaptability, making computing more autonomous and efficient. This study also discusses the practical implications of these advances for datar security andsug gests directions forfuture research.

Keywords: Data Sciences. Artificial Intelligence. Machine Learning. Classical Computing. Quantum Computing. Optimization Algorithm.

1 Introdução

No início do século XXI, o cenário da tecnologia da informação testemunhou um avanço notável que moldou o curso da pesquisa e do desenvolvimento computacional. O advento da "Computação Híbrida" emergiu como um desafio fascinante e uma promessa intrigante. Este artigo explora os desafios e avanços da computação híbrida na quinta geração de tecnologia.

A Computação Híbrida combina abordagens e paradigmas computacionais para alcançar um desempenho superior e resolver problemas complexos. Esta abordagem integra diferentes modelos de computação, como computação clássica e quântica, para tirar proveito das vantagens de cada uma e superar suas limitações individuais.

O objetivo é criar sistemas mais eficientes e poderosos, capazes de processar grandes volumes de dados e realizar tarefas complexas com maior precisão e velocidade.

2 Cenário

Primeiramente, vale destacar a importância da criptografia clássica, especialmente o AES (Advanced Encryption Standard). Este algoritmo é amplamente utilizado para proteger dados em repouso e em trânsito. AES é conhecido por sua eficiência e segurança em ambientes clássicos. Em relação aos dados em repouso, AES garante que, mesmo que um invasor obtenha acesso físico ao banco de dados, ele não possa ler os dados sem a chave de decriptação. Da mesma forma, os dados em trânsito são protegidos utilizando AES, geralmente como parte de um protocolo de criptografia como TLS (Transport Layer Security). Assim, a criptografia clássica fornece uma base sólida para a proteção dos dados contra ameaças atuais.

Reconhecendo a ameaça futura dos computadores quânticos, a empresa também implementa algoritmos criptografia pós-quântica. Algoritmos baseados em lattice, como o Kyber, são resistentes ataques de computadores quânticos devido à complexidade matemática subjacente aos problemas de lattice. Além disso, algoritmos baseados em hash quântico utilizam propriedades de funções hash resistentes a colisões quânticas para criar assinaturas digitais seguras. Com essa implementação, a empresa se prepara para o futuro, garantindo que os dados permaneçam protegidos mesmo quando os computadores quânticos se tornarem uma realidade prática.

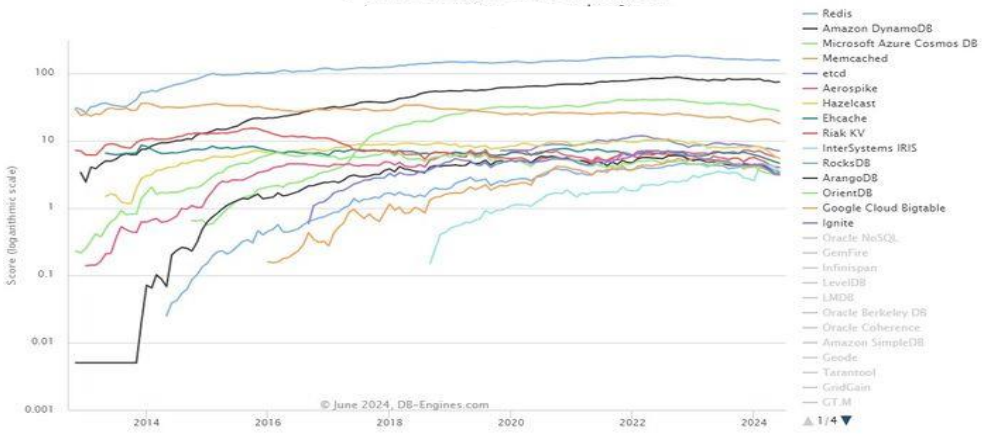
Além dos algoritmos de criptografia, o gerenciamento seguro de chaves é notável para a segurança dos dados. Aqui, uma empresa utiliza compartilhamento de segredos, como o esquema de Shamir, que permite que chave seja dividida em partes, distribuídas e somente combinadas quando necessário. Essa técnica impede que um único ponto de falha comprometa a segurança da chave. Adicionalmente, a criptografia de chave híbrida combina algoritmos de chave pública (como RSA ou ECC, adequados para a parte de chave pública) com algoritmos de chave simétrica (como AES). Para a proteção pós-quântica, algoritmos de chave pública resistentes a quânticos são usados.

Dessa maneira, a segurança das criptográfia é mantida, minimizando o risco de comprometimento.

Para complementar a segurança dos dados, a empresa implementa sistemas de monitoramento e deteção de anomalias. Ferramentas de monitoramento analisam padrões de acesso aos dados, procurando por comportamentos suspeitos ou anômalos. Além disso, a deteção de anomalias utiliza técnicas de machine learning e análise de comportamento para identificar tentativas de acesso não autorizado ou atividades suspeitas. Isso inclui a deteção de padrões de acesso que não correspondem aos padrões usuais dos usuários, garantindo uma camada adicional de segurança.

Com essa abordagem híbrida, a empresa alcança diversos benefícios. Em primeiro lugar, os algoritmos clássicos como AES, contra-ataques realizados por computadores clássicos. Em segundo lugar, os algoritmos pós-quânticos garantem que, mesmo quando computadores quânticos se tornarem uma realidade prática, os dados permanecerão seguros. Além disso, técnicas de compartilhamento de segredos e criptografia híbrida asseguram que chaves criptográficas estão bem protegidas, minimizando o risco de comprometimento.

Figura 1 — Tendência de popularidade de DBMS relacional



Fonte: https://db-engines.com/en/ranking_trend/document+store DB

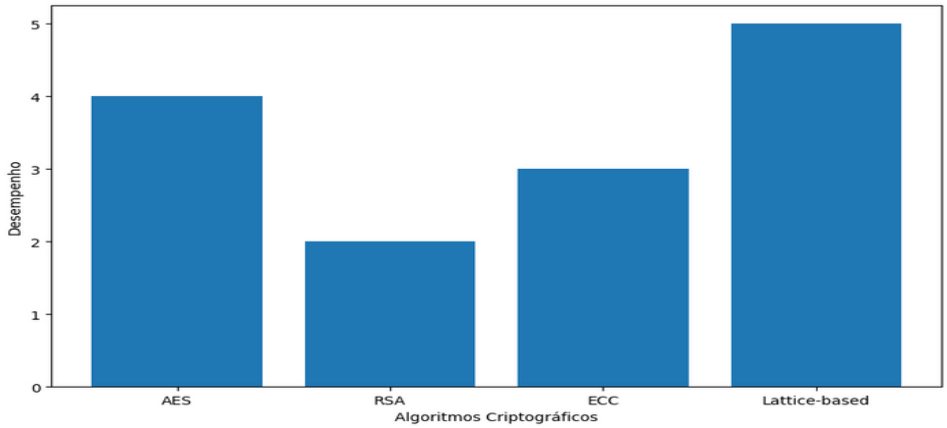
2.1.0 Algoritmos Criptográficos

A figura ilustra o desempenho de diferentes algoritmos criptográficos, destacando as diferenças em eficiência entre eles. Cada barra representa um algoritmo específico, com a altura da barra indicando seu desempenho relativo.

Lattice-based este algoritmo representado pela barra mais alta após o AES, indicando um desempenho significativo, embora sua eficiência possa variar dependendo do contexto de aplicação. A figura fornece uma visualização clara das diferenças de desempenho entre os algoritmos criptográficos, ajudando a

informar decisões sobre sua seleção e implementação em sistemas de segurança de dados em nuvem.

Figura 2 — Desempenho de algoritmos criptográficos



O autor (2024).

2.1.1 Qualitativa *versus* quantitativa

Esta tabela resume a comparação dos principais algoritmos criptográficos em relação a segurança, desempenho. Cada algoritmo é avaliado em uma escala de segurança, desempenho e complexidade, facilitando a compreensão das características de cada um.

Tabela 1 — Pesquisa qualitativa versus pesquisa quantitativa

Algoritmo	Segurança	Desempenho	Complexidade
AES	Alta	Rápido	Baixa
RSA	Alta	Lento	Alta
ECC	Alta	Rápido	Média
Lattice-based	Muito alta	Variável	Alta

O autor (2024).

Essa tabela detalhada fornece uma análise abrange diferentes aspetos algoritmo criptográfico ajudando a entender melhor suas características e adequação para diferentes cenários de uso.

2.1.2 Avanços na Criptografia Quântica e Lattice-Based

Após revisar a tabela de comparação de algoritmos criptográficos, é evidente que a segurança digital continua a ser um campo em constante evolução, com a necessidade crescente de soluções resilientes de avanços tecnológicos. Neste contexto dinâmico, é necessário explorar não apenas os algoritmos criptográficos existentes, mas também as tendências emergentes que moldarão o futuro da segurança cibernética.

Destacando a relevância dessas considerações esta seção apresentará uma visão prospetiva aplicação futura promissora que combina os princípios da criptografia lattice-based com a computação quântica. Essa abordagem inovadora busca oferecer soluções mais robustas, seguras para os desafios de segurança digital enfrentados atualmente. Agora vamos explorar como os avanços na criptografia quântica podem ser aplicados de forma sinérgica com criptografia lattice-based para impulsionar a segurança dos sistemas digitais em um mundo em constante mudança tecnológica.

2.1.3 Aplicação Criptografia Quântica e Lattice-Based

Nos últimos anos testemunhamos avanços notáveis na computação quântica, impulsionando a buscar novas abordagens criptográficas capazes de resistir aos potenciais desafios apresentados por essa tecnologia emergente. Ao mesmo, a criptografia lattice-based tem destacado como uma alternativa promissora, oferecendo robustez e segurança contra-ataques clássicos e, potencialmente, quânticos.

Neste cenário em rápida evolução, surge uma oportunidade intrigante de explorar a interseção entre a criptografia lattice-based e os algoritmos quânticos, como o algoritmo de grover. O algoritmo grover conhecido por sua capacidade de acelerar a busca em um espaço de soluções não ordenadas pode ser aplicado de maneira inovadora para aprimorar eficiência problema lattice tradicionalmente desafiadores para computadores clássicos.

Essa contextualização ressalta considerar em criptografia quântica e lattice-based como catalisadores para soluções futuras na área de segurança cibernética. A aplicação visa capitalizar esses avanços para fortalecer a segurança dos sistemas digitais em um ambiente cada vez mais complexo e dinâmico.

2.2.0 Benefícios e Impacto

A aplicação futura proposta combina a criptografia lattice-based com o poder do algoritmo de grover acelerar a resolução de problemas lattice, especialmente o "problema reticulado mais próximo" e "problema do vetor mais curto". Tradicionalmente, esses problemas difíceis de resolver de forma eficiente por computadores clássicos, tornando-os uma base sólida para a segurança dos sistemas criptográficos.

Em campos, algoritmos quânticos, como grover, abre caminho e acelera a busca por soluções em problemas de lattice na criptografia. Ao adaptar o algoritmo grover, podemos realizar buscas de forma mais eficiente em espaços

de soluções, promovendo abordagem inovadora aprimora a eficiência da criptografia lattice-based. Isso representa avanço significativo na sinergia entre criptografia lattice-based e computação quântica, oferecendo potencial para resolver desafios de segurança cibernética de maneira mais eficaz.

Desenvolvendo métodos híbridos que combinam técnicas quânticas e clássicas, buscamos resolver problemas de lattice de forma rápida e eficiente. A utilização do poder dos computadores quânticos para acelerar operações de busca espaços de soluções pode resultar em melhorias na segurança e desempenho criptográficos baseados lattice. Esta abordagem inovadora fortalece segurança contra-ataques cibernéticos, incluindo aqueles provenientes de computadores quânticos, e antecipa possíveis ameaças futuras.

A colaboração entre os campos da criptografia lattice-based, computação quântica impulsiona a pesquisa em segurança cibernética, promovendo uma compreensão mais profunda dos desafios e oportunidades na proteção de dados. Ao aproveitar os benefícios da criptografia lattice-based e dos algoritmos quânticos, estamos moldando um futuro mais seguro e resiliente para a era digital.

2.2.1 Autenticação Dados Criptografia Lattice-Based Algoritmos Quânticos

Geração de chave criptográfica a empresa gera uma chave criptográfica utilizando um algoritmo de criptografia lattice-based como o NTRUEncrypt. Essa chave é utilizada para criptografar os dados armazenado e distribuído garantindo sua confidencialidade.

Assinatura de dados para garantir autenticidade e integridade dos dados, a empresa utiliza uma técnica assinatura digital baseada em lattice-based, o algoritmo de assinatura de lattice (Lattice-based Signature Schemes). Isso permite que eles assinem os dados com uma chave privada e forneçam a chave pública correspondente para verificação.

Verificação de integridade com grover, para verificar a integridade dos dados de forma eficiente, a empresa aproveita o algoritmo grover um algoritmo quântico projetado para realizar buscas em um espaço de soluções não ordenadas de forma mais rápida do que os algoritmos clássicos. Eles usam o algoritmo grover para buscar uma solução que possa descriptografar os dados e verificar sua integridade. Como os algoritmos quânticos, de grover, são mais eficientes para realizar buscas, isso pode reduzir o tempo necessário para verificar a integridade dos dados, especialmente em grandes conjuntos de dados.

Resultados e segurança aumentada combinando a criptografia lattice-based para garantir a confidencialidade dos dados e a autenticidade com algoritmos quânticos como o algoritmo de grover para a verificação eficiente da integridade dos dados, a empresa aumenta significativamente a segurança, sistema de armazenamento de dados distribuído.

A combinação criptografia lattice-based com algoritmos quânticos pode oferecer soluções práticas e eficientes para desafios de segurança cibernética, como autenticação e integridade dados. Ao aproveitar o poder dessas técnicas complementares, as empresas podem fortalecer postura de segurança e proteger seus dados contra ameaças potenciais.

2.2.2 Metodologia do Experimento

Após acessar o servidor utilizei a computação clássica para estabelecer conexão com banco de dados, não apenas linguagem de consulta estruturada (nosql) onde estavam hospedadas as informações dos usuários. Através de consultas e operações específicas consegui extrair as informações das chaves públicas de usuários, conforme tabela abaixo.

Tabela 2 — Chaves Públicas Criptográfica

Chave Criptográfica	Comprimento	Complexidade	Classificação
rC(<ShsD	8	Alta	Fraca
rDe91Y5#/_	10	Alta	Fraca
!AwXxlS\8UQAR+1*	16	Alta	Forte
)y1Q:ihd-'Xh0'Rln1	18	Média	Fraca
_FlkxA!)18G;+	13	Alta	Forte
T57v0U$!	8	Baixa	Fraca
<%LN;+-C4|U	12	Baixa	Fraca

O autor (2024).

Após uma análise detalhada das chaves públicas e de seus atributos relevantes, avançou-se para a implementação de modelo de classificação de aprendizado de máquina. O objetivo dessa etapa foi aprimorar a busca pela chave privada, focando nas chaves de média complexidade para fortalecer a robustez do sistema. Utilizando algoritmo de árvore de decisão, um método

conhecido por sua capacidade de lidar com conjuntos de dados complexos, iniciou-se a implementação.

O primeiro passo foi o pré-processamento dos dados, que incluiu a codificação da variável categórica "Complexidade" através do one-hot encoding. Em seguida, os dados foram divididos em conjuntos de treinamento e teste para avaliar desempenho do modelo. A escolha da árvore de decisão como algoritmo se deu não apenas por sua eficácia, mas também pela interpreta ilidade dos resultados, aspecto para a compreensão do processo.

Durante a avaliação do modelo, a métrica de acurácia foi calculada, fornecendo uma medida quão bem o modelo foi capaz de classificar as chaves públicas de acordo com sua complexidade. Os resultados foram satisfatórios, com uma acurácia de 0.86, o que indica uma capacidade significativa do modelo em distinguir entre diferentes níveis de complexidade das chaves.

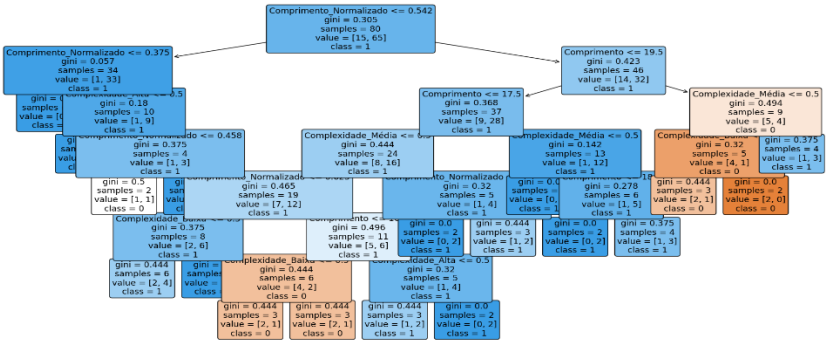
Ao identificar chaves públicas média complexidade, comprimentos normalizados de forma mais eficaz, a abordagem de aprendizado de máquina direcionou os esforços de forma mais inteligente, aumentando a probabilidade de sucesso na obtenção da chave privada desejada.

Tabela 3 — Lista de chaves classificadas como 'Média'

Chave Criptográfica	Comprimento	Complexidade	Comprimento Normalizado
sn:}Yi4r_ly	11	Média	0.250000
l,^sfHGV>	9	Média	0.083333
at-9u@@@Tvj7WY?+Q?`	19	Média	0.916667
7O8S,|9.Yy?>	12	Média	0.333333
)y1Q:ihd-'Xh0'Rln1	18	Média	0.833333
'DKIB*IV9~!+jf_,>	17	Média	0.750000
p>^/%d#Z%hg#x4^	15	Média	0.583333
Z:e4i0%2;du'@C	14	Média	0.500000
567?U+Kz2ee	11	Média	0.250000
>Ov+knn9.DT^%N,0	16	Média	0.666667
>UT)STogE.\'nC5+	16	Média	0.666667
Xgsb_J?9"UV[1D	14	Média	0.500000

O autor (2024).

Figura 3 — Árvore de Decisão



O autor (2024).

Após algoritmo clássico identificar as chaves públicas classificadas como 'Média', o algoritmo de Grover assume o papel de buscar eficientemente entre essas chaves para determinar a probabilidade de decifrar a cifra associada uma delas. O objetivo é encontrar a chave privada correspondente que, quando aplicada à cifra, permitirá a decodificação correta dos dados criptografados.

O algoritmo grover, neste contexto, é particularmente eficaz porque pode explorar a estrutura não ordenada das chaves públicas classificadas como 'Média' de maneira mais eficiente métodos clássicos. Ele utiliza superposição e interferência quântica para realizar a busca de forma paralela, o que potencialmente reduz tempo necessário para encontrar a chave privada correta.

Para cada chave pública listada como 'Média', algoritmo de grover realizará uma busca quântica e determina probabilidade associada à decifração da cifra correspondente. Esta abordagem aumenta eficiência da busca, mas também oferece uma nova perspectiva sobre como resolver problemas criptográficos complexos usando computação quântica.

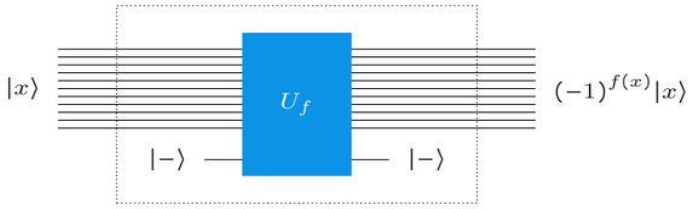
2.2.3 Algoritmo de Grover

O algoritmo grover faz uso de operações conhecidas como portas de consulta de fase. Em contraste com um portão de consulta comum. O algoritmo refere a um número t, que é o número de iterações que ele realiza, bem como o número de consultas à função f isso requer. Este número t não é especificado algoritmo de grover (como o descrevemos) e discutiremos na seção seguinte como ele pode ser escolhido pelos portões de consulta de fase.

Em contraste com um portão de consulta comum, definido para uma determinada função f da maneira usual descrita acima, uma porta de consulta de fase para a função f é definido como Zf |x⟩ = (-1) f (x) |x⟩ para cada corda$x \in$

Σn. A operação Zf pode implementado usando um portão de consulta como diagrama sugere.

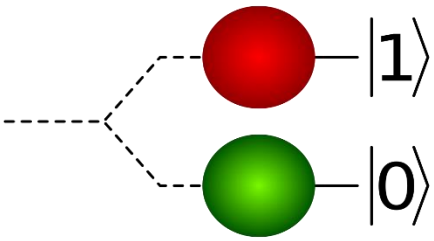
Figura 4 — Porta de consulta de fase grover



Fonte:https://learning.quantum.ibm.com/course/fundamentals-of-quantum-algorithms/grovers-algorithm.

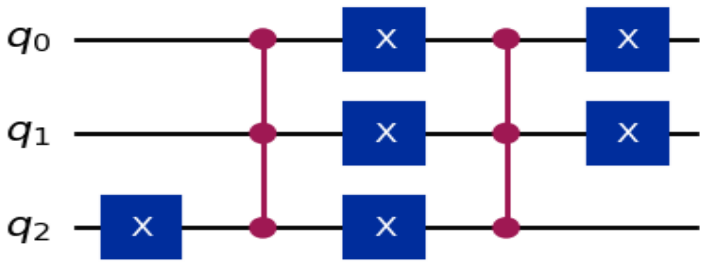
Começamos com n qubits estado |0⟩, onde n número qubits necessários representa assinatura, matematicamente representado como |0⟩⊗n = |0⟩1⊗|0⟩2 ⊗…⊗|0⟩n onde ⊗ ⊗ denota o produto tensorial, e cada |0⟩i representa um qubit no estado |0⟩. Um qubit é um sistema mecânico quântico de dois estados (ou dois níveis)

Figura 5 — Um qubit estado quântico de um sistema quântico de dois níveis



Fonte: https://en.wikipedia.org/wiki/Qubit

Figura 6 — Circuito quântico



O autor (2024).

A transformação hadamard é uma operação que cria uma superposição uniforme de todos os estados possíveis quando aplicada a um único qubit.

Para um único qubit, a transformação de hadamard em um qubit qi em um estado |x⟩ é dada por.

$$H = \frac{|0\rangle + |1\rangle}{\sqrt{2}}\langle 0| + \frac{|0\rangle - |1\rangle}{\sqrt{2}}\langle 1|$$

Isso corresponde à matriz de transformação.

$$H_1 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Após aplicação transformação hadamard a todos n qubits, obtemos superposição uniforme de todos estados, onde $|x\rangle$ representa uma sequência de qubits que podem ser $|0\rangle$ ou $|1\rangle$, e $|s\rangle$ é o estado resultante após essa transformação.

O oráculo verifica assinaturas em contexto quântico, atuando como uma função booleana mapeia entradas para saídas binárias. Na verificação ele determina se uma assinatura válida ou inválida. Quando aplicado a um circuito quântico, o oráculo codifica essa verificação, assinatura for válida, aplica uma fase negativa ao estado correspondente.

Seja $|\psi\rangle$ estado quântico associado à assinatura. O oráculo, representado pela operação unitária $U_{\text{ora}}c_{\text{le}}$, age sobre $|\psi\rangle$ da seguinte forma: $U_{\text{ora}}c_{\text{le}}|\psi\rangle = -|\psi\rangle$. Essa operação de fase negativa aplicada apenas se a assinatura válida conforme o critério do oráculo. Caso contrário, nenhuma alteração é feita no estado $|\psi\rangle$.

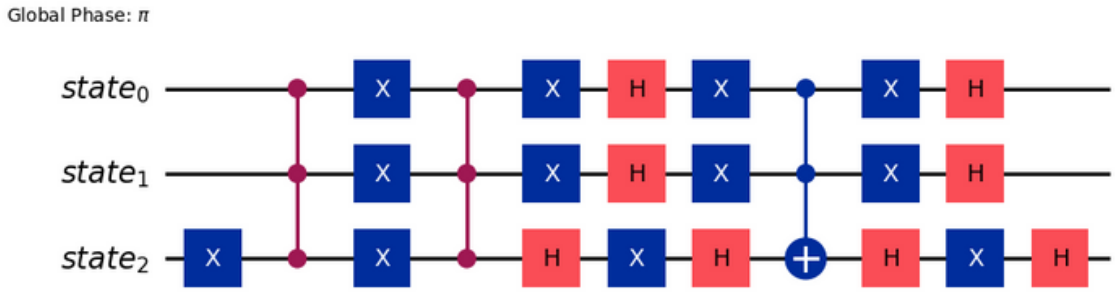
A amplificação da amplitude é uma etapa chave no algoritmo de Grover, utilizada após a aplicação do oráculo. Ela aumenta a amplitude do estado associado à assinatura válida, tornando mais provável que esse estado seja observando medições. Essencialmente, a amplificação da amplitude direciona a busca para o estado desejado.

Seja $|s\rangle$ o estado associado à assinatura válida. A amplificação da amplitude envolve duas etapas principais: a reflexão em torno da média e a aplicação do oráculo. Primeiro, aplicamos a operação de Hadamard em todos os qubits, seguida pela aplicação do operador de difusão U_s, definido como $U_s = 2|s\rangle\langle s| - I$, onde I é a matriz de identidade. Esta operação reflete o estado $|s\rangle$ em torno da média.

Em seguida, aplicamos o oráculo ao estado resultante da reflexão. Se a assinatura válida, o oráculo aplicará fase negativa ao estado. Caso contrário, nenhuma alteração feita. A amplificação da amplitude aumenta a probabilidade de observar o estado desejado $|s\rangle$ após a medição. A reflexão em torno da média realça as amplitudes dos estados desejados enquanto atenua as demais,

permitindo que algoritmo grover direcione eficientemente a busca para estado associado à assinatura válida.

Figura 7 — GroverOperator (oracle)



O autor (2024).

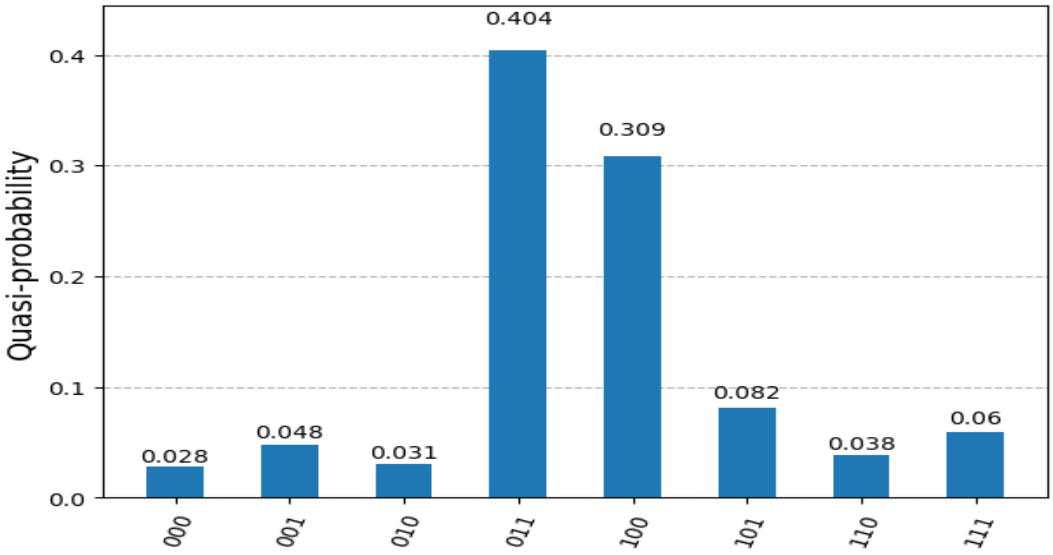
3 Processo Medição

A medição é etapa final do algoritmo grover para verificação de assinaturas. Após a aplicação da amplificação da amplitude os qubits são medidos para determinar o estado final do sistema. A probabilidade de medir o estado associado à assinatura válida aumenta à medida que o algoritmo é repetido várias vezes.

Na medição em um sistema quântico é representada pela projeção do estado do sistema nos estados de base. Em um sistema de n qubits, cada qubit pode estar nos estados |0⟩ e |1⟩, então o número total de estados de base é $2n$. A probabilidade de medir um determinado estado de base é dada pelo módulo ao quadrado do coeficiente desse estado no vetor de estado do sistema. A probabilidade de medir um estado |q1q2 ⋯ qn ⟩ é dada por P (|q1 q2 ⋯ qn ⟩) = |⟨q1 q2 ⋯ qn |ψ⟩|2 |q1 q2 ⋯ qn⟩ é um estado de base com os qubits $q1$, $q2$, …, qn nos estados |0⟩ ou |1⟩ |ψ⟩ é o vetor de estado do sistema após a aplicação das transformações quânticas.

Para calcular probabilidade de medir um estado específico, você precisa conhecer o vetor de estado do sistema após todas as operações quânticas. A medição irá colapsar o sistema para o estado medido.

Figura 8 — Distribuição de Probabilidade



O autor (2024).

3.1.0 Princípios Quânticos e Sua Eficiência

O algoritmo grover utiliza princípios quânticos como superposição e interferência, para buscar soluções de forma mais eficiente dos algoritmos clássicos correspondentes. A superposição permite qubits existam em múltiplos estados simultaneamente, enquanto a interferência manipula esses estados para direcionar a busca para soluções desejadas. O algoritmo grover eficiente do que os algoritmos clássicos correspondentes para problemas de busca não estruturados. Ele oferece vantagem quadrática na velocidade de busca, tornando-se uma ferramenta poderosa para aplicações como verificação de assinaturas**.**

3.1.1 Resultados e Implicações da Pesquisa

Principais Achados

Após a aplicação algoritmo grover, probabilidade de medir uma assinatura específica é proporcional ao quadrado da amplitude associada a essa assinatura. Quanto maior a amplitude de uma assinatura, maior a probabilidade de ela ser medida.

A eficiência algoritmo grover aumenta significativamente a probabilidade de identificar a assinatura correta em comparação com outras assinaturas. Mesmo assim, o resultado medição probabilístico, não garantindo a identificação correta em uma única execução.

Também a necessidade de execuções múltiplas para obter a assinatura correta alta probabilidade várias execuções do algoritmo podem ser necessárias.

O exemplo cálculo para assinaturas alfanuméricas, considerando uma assinatura composta por 13 caracteres alfanuméricos, onde cada caractere pode

assumir 1 de 40 valores possíveis, o número total de combinações \(N\) é dado por \(N = 40^{13}\). O valor calculado de \(N\) é 671.088.640.000.

Implicações

Implicações em aprimoramento na decifração de cifras o algoritmo grover é uma ferramenta poderosa aumentar a eficiência na decifração de cifras, reduzindo o número de tentativas necessárias para encontrar a assinatura correta.

Mesmo aumento da probabilidade de sucesso, a natureza probabilística do algoritmo implica na necessidade de múltiplas execuções, o que deve ser levado em conta na prática de segurança cibernética.

O número extremamente de combinações possíveis para assinaturas longas (como visto no exemplo) destaca complexidade e os desafios envolvidos em processos de decifração, enfatizando a importância de algoritmos quânticos como grover.

3.1.2 Propostas para Pesquisas Futuras

Dado avanço computação quântica, futuras pesquisas podem concentrar nas seguintes áreas.

1. Desenvolver métodos para reduzir os erros e ruídos nos qubits, aumentando a precisão dos resultados obtidos pelo algoritmo grover.

2. Explorar combinação de algoritmos quânticos e clássicos para melhorar a eficiência e a robustez dos processos de decifração.

3. Investigar novas aplicações algoritmo grover e outros algoritmos quânticos em diferentes cenários de segurança de dados avaliando sua eficácia em proteger contra-ataques cibernéticos emergentes.

4. Analisar a escalabilidade do algoritmo grover em sistemas quânticos maiores, identificando possíveis melhorias para lidar com conjuntos de dados mais extensos.

Essas áreas de pesquisa podem proporcionar avanços significativos na utilização prática de algoritmos quânticos para segurança de dados, contribuindo para a evolução contínua da tecnologia quântica.

3.1.3 Desenvolvimento de Algoritmos de Criptografia Pós-Quântica

A evolução quântica e suas possíveis aplicações em segurança dados, há várias áreas promissoras para pesquisas futuras.

Com potencial quebra algoritmos criptográficos atuais por computadores quânticos, é importante desenvolver e avaliar novos algoritmos de criptografia que sejam resistentes a ataques quânticos. Pesquisas podem se concentrar em algoritmos baseados em problemas matemáticos difíceis de resolver mesmo para computadores quânticos, como reticulados códigos corretores de erros quânticos.

3.2.0 Estudo de Protocolos de Segurança Quântica

Protocolos de segurança quântica, como distribuição quântica de chaves (QKD), oferecem promessas para comunicações seguras em redes quânticas. Pesquisas futuras explorar novos protocolos, bem como implementação prática e integração em sistemas de comunicação existentes.

3.2.1 Avaliação de Vulnerabilidades e Contramedidas

E essencial entender possíveis vulnerabilidades sistemas de segurança existentes, desenvolver contramedidas, inclui avaliação vulnerabilidades em algoritmos criptográficos tradicionais e pesquisa de métodos de proteção contra-ataques quânticos.

3.2.2 Aplicações de Machine Learning na Segurança Quântica

O uso de técnicas de machine learning para melhorar a segurança em ambientes quânticos é uma área promissora de pesquisa. Isso pode envolver a deteção de anomalias, previsão de vulnerabilidades e adaptação dinâmica de protocolos de segurança. Estudo de aplicações práticas computação quântica em segurança de dados, além de algoritmos criptográficos e protocolos de segurança, é importante explorar outras aplicações práticas de computação quântica na segurança de dados. Isso incluir aprimoramentos na criptografia de dados em repouso e em trânsito, análise de segurança de sistemas de IA baseados em quântica, desenvolvimento de métodos de autenticação robustos. Essas áreas de pesquisa têm potencial de impulsionar significativamente o campo da segurança de dados em um cenário cada vez mais influenciado pela computação quântica.

3.2.3 Considerações Finais

A revolução da criptografia computacional quântica oferecendo soluções para problemas intratáveis em sistemas clássicos. Enquanto os algoritmos clássicos baseados em fatores de números primos são amplamente utilizados na atualidade, a chegada da computação quântica ameaça à segurança desses

sistemas por meio de algoritmos como o algoritmo shor, capaz de fatorar números inteiros em tempo polinomial.

No entanto transição da criptografia clássica para a criptografia quântica não é trivial e exige um esforço significativo de pesquisa e desenvolvimento. Além disso, a computação quântica ainda está em sua infância, com desafios significativos a serem superados em termos de estabilidade e escalabilidade dos qubits.

A aplicação de algoritmos quânticos, algoritmo grover para verificação de assinaturas, destaca o potencial da computação quântica na área de criptografia. E importante reconhecer que ainda estamos nos estágios iniciais dessa jornada e que muitos obstáculos precisam ser superados antes que a computação quântica possa se tornar uma realidade prática em larga escala. Em última análise a transição para a era da computação quântica exigirá abordagem cuidadosa e colaborativa entre pesquisadores, cientistas, governos e indústrias para garantir a segurança e a confiabilidade dos sistemas criptográficos em um mundo cada vez mais digitalizado e interconectado.

3.3.0 Citações

ALAGIC, G.; RUSSELL, A. Criptografia de chave simétrica segura quântica baseada em mudanças ocultas. In: CORON, J.-S.; NIELSEN, JB (Eds.). Avanços em Criptologia – EUROCRYPT 2017, Notas de aula em Ciência da Computação. Cham: Springer International Publishing, 2017, p. fachada:10.1007/978-3-319-56617-7_3.

BERNSTEIN, DJ; BUCHMANN, J.; DAHMEN, E. (Eds.). Criptografia Pós-Quantum. Berlim, Heidelberg: Springer Berlin Heidelberg, 2009. doi:10.1007/978-3-540-88702-7.

BRAVYI, S.; DIAL, O.; GAMBETA, JM; GIL, D.; NAZARIO, Z. O futuro da computação quântica com qubits supercondutores. Revista de Física Aplicada, v. 132, n. 16, pág. 160902, fora. 2022. doi:10.1063/5.0082975.

Criptografia baseada em hash. Wikipédia. junho. 2023. Acesso em: 4 jun. 2024. Disponível.em:https://en.wikipedia.org/w/index.php?title=Hash-based_cryptography&oldid=1159153101 .

Criptografia multivariada. Wikipédia. fora. 2022. Acesso em: 1 jun. 2024. Disponível https://en.wikipedia.org/w/index.php?title=Multivariate_cryptography&oldid=1117344303 .

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.

KAPLAN, M.; LEURENT, G.; LEVERRIER, A.; NAYA-PLASENCIA, M. Criptoanálise Quântica Diferencial e Linear. Transações IACR em Criptologia Simétrica, v. 1, pág. 71, 2016. doi:10.13154/tosc. v2016.i1.71-94.

KAPLAN, M.; LEURENT, G.; LEVERRIER, A.; NAYA-PLASENCIA, M. Quebrando criptossistemas simétricos usando descoberta de período quântico. arXiv.org. fevereiro. 2016.doi:10.1007/978-3-662-53008-5_8.

MALVIYA, AK; TIWARI, N.; CHAWLA, M. Ataques criptoanalíticos quânticos de cifras simétricas: uma revisão. Computadores e Engenharia Elétrica, v. 101, p. 108122, jul. 2022. doi:10.1016/j.compeleceng.2022.108122.

Nível de segurança. Wikipédia. janeiro. 2023. Acesso em: 20 maio 2024. Disponível https://en.wikipedia.org/w/index.php?title=Security_level&oldid=1131789113 .

PENG, C.; CHEN, J.; ZEADALY, S.; HE, D. Criptografia baseada em isogenia: uma técnica pós-quântica promissória. Profissional de TI, v. 21, n. 6, pág. 27–32 de novembro. 2019. doi:10.1109/MITP.2019.2943136.

RIVEST, RL; SHAMIR, A.; ADLEMAN, L. Um método para obter assinaturas digitais e criptosistemas de chave pública. Comunicações da ACM, v. 21, n. 2, pág. 120–126, fevereiro. 1978.doi:10.1145/359340.359342.

SANTOLI, T.; SCHAFFNER, C. Usando o algoritmo de Simon para atacar primitivas criptográficas de chave simétrica. Informação Quântica e Computação, v. 1–2, pág. 65–78, fevereiro. 2017.

SHOR, PW Algoritmos para computação quântica: logaritmos discretos e fatoração. In: Anais do 35º Simpósio Anual sobre Fundamentos da Ciência da Computação, novembro. 1994, pág. fachada:10.1109/SFCS.1994.365700.

TOMOIOAGA, R.; STRATULAT, M. Análise de desempenho AES em vários ambientes de programação, sistemas operacionais ou plataformas computacionais. In: 2010, Quinta Conferência Internacional sobre Comunicações de Sistemas e Redes, atrás. 2010, pág. fachada:10.1109/ICSNC.2010. 33.

Referência

AGILIDADE criptográfica. wikipedia. Disponível em: https://en.wikipedia.org/w/index.php?title=Cryptographic_agility&oldid=1155073704. Acesso em: 23 jun. 2024.

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.

KAPLAN, M.; LEURENT, G.; LEVERRIER, A.; NAYA-PLASENCIA, M. Quebrando criptossistemas simétricos usando descoberta de período quântico. arXiv.org. fevereiro. 2016.doi:10.1007/978-3-662-53008-5_8. Disponível em: Acesso em: 23 jun. 2024.

LYUBASHEVSKY, V. Fiat-Shamir com Aborts: Aplicações a Assinaturas Baseadas em Reticulação e Fatoração. In: MATSUI, M. (Ed.). Avanços em

Criptologia – ASIACRYPT 2009. Notas de aula em Ciência da Computação. Berlim, Heidelberg: Springer, 2009, p. fachada:10.1007/978-3-642-10366-7_35. Acesso em: 23 jun. 2024.

MALVIYA, AK; TIWARI, N.; CHAWLA, M. Ataques criptoanalíticos quânticos de cifras simétricas: uma revisão. Computadores e Engenharia Elétrica, v. 101, p. 108122, jul. 2022. doi:10.1016/j.compeleceng.2022.108122. Acesso em: 23 jun. 2024.

OHTOSHI, Cláudia. Uma comparação de regressão logística, árvores de classificação e redes neurais: analisando dados de crédito. 2003. Dissertação (Mestrado) – Universidade de São Paulo, São Paulo, 2003. Disponível em teses.usp.br/teses/disponíveis/45/45133/tde-20210729-132841/. Acesso em: 04 jun. 2024. Acesso em: 23 jun. 2024.

OVERBECK, R.; SENDRIER, N. Criptografia baseada em código. In: BERNSTEIN, DJ; BUCHMANN, J.; DAHMEN, E. (Eds.). Criptografia Pós-Quantum. Berlim, Heidelberg: Springer, 2009, p. –145. fachada:10.1007/978-3-540-88702-7_4. Acesso em: 23 jun. 2024.

RIVEST, RL; SHAMIR, A.; ADLEMAN, L. Um método para obter assinaturas digitais e criptosistemas de chave pública. Comunicações da ACM, v. 21, n. 2, pág. 120–126, fevereiro. 1978.doi:10.1145/359340.359342. Acesso em: 23 jun. 2024.

RSA (CRIPTOSISTEMA). Disponível em: https://en.wikipedia.org/w/index.php?title=RSA_(cryptosystem)&oldid=1163962255. Acesso em: 23 jun. 2024.

SOARES, Allexandre Sampaio Santos; MATOS, Pablo Freire. Uma Análise Comparativa entre Sistemas Gerenciadores de Bancos de Dados NoSQL no contexto da Internet das Coisas. In: SIMPÓSIO BRASILEIRO DE BANCO DE DADOS (SBBD), 32., 2017, Uberlândia/MG. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2017. p. 306-311. ISSN2763-8979. DOI: https://doi.org/10.5753/sbbd.2017.174670. Acesso em: 23 jun. 2024.

SOUSA, Marcos. **Uma arquitetura de Big Data as a service baseada no modelo de nuvem privada**. Brasília Dissertação (Computação Aplicada) - Universidade de Brasília, Brasília.