Os Impactos do Algoritmo de Grover na Segurança da Criptografia Simétrica: Uma Análise da Redução de Entropia no Padrão AES.

Eduardo Lordão Oliveira[1], **Evellyn Fernanda Alamin Machado**[1], **Giullia Rodrigues de Menezes**[1]

[1]Faculdade de Computação - Universidade Federal de Uberlândia (UFU)
Caixa Postal 38408-100 – Uberlândia – MG – Brasil

{eduardo.lordao, evellyn.machado, giullia.rodrigues}@ufu.br

Abstract. *This expanded abstract analyzes the reduction of the security margin in symmetric-key algorithms due to advancements in quantum computing, focusing specifically on the logical and mathematical framework of Grover's Algorithm. The primary objective is to demonstrate how the quadratic speedup, represented by the complexity $O(\sqrt{N})$ in unstructured database searches, compromises widely used cryptographic standards such as AES-128. Through a theoretical analysis and a proposed implementation via IBM Qiskit, this study demonstrates that the quantum computational advantage necessitates an immediate migration to 256-bit keys to maintain robustness against brute-force attacks in the post-quantum era.*

Resumo. *Este resumo expandido analisa a redução da margem de segurança em algoritmos de chaves simétricas pelo avanço da computação quântica, focando especificamente no funcionamento lógico e matemático do Algoritmo de Grover. O objetivo principal é mostrar como a aceleração quadrática $(O(\sqrt{N}))$ na busca em bases de dados não ordenadas compromete padrões criptográficos que são muito utilizados nos dias de hoje, como o AES-128. Por meio de uma análise teórica e proposta de implementação via IBM Qiskit, demonstra-se que a vantagem computacional quântica exige a migração imediata para chaves de 256 bits a fim de manter a robustez contra ataques de força bruta na era pós-quântica.*

1. Introdução

A segurança da infraestrutura digital depende, em grande parte, da dificuldade computacional de ataques de *Brute Force* contra algoritmos de criptografia simétrica, como o Advanced Encryption Standard (AES). Em computadores clássicos, a busca por uma chave em um espaço de tamanho N requer, em média, $N/2$ tentativas, resultando em complexidade $O(N)$ [Stallings 2017].

Com o avanço da computação quântica, surgem novos modelos de processamento baseados em superposição e entrelaçamento de estados. Nesse contexto, o Algoritmo de Grover permite realizar buscas em bases não ordenadas com maior eficiência, reduzindo a complexidade para aproximadamente $\sqrt{N}$ operações.

Essa aceleração quadrática reduz a segurança efetiva de chaves simétricas pela metade, o que levanta preocupações sobre a segurança dos sistemas atuais. Assim, este

artigo apresenta uma análise do funcionamento do Algoritmo de Grover e discute seus impactos na segurança de padrões criptográficos, como o AES-128, o que demonstra a importância do uso de chaves maiores, como no AES-256.

2. Fundamentação Teórica e Modelagem Automática

Nesta seção, o Algoritmo de Grover é descrito como a manipulação de vetores em um espaço de Hilbert de $N = 2^n$ dimensões, onde n é o número de qubits [Grover 1996].

2.1. Representação de Estados e Inicialização

O algoritmo inicia com o sistema no estado fundamental $|0\rangle^{\otimes n}$. Para explorar o paralelismo quântico, é aplicado uma transformação de Hadamard (H) em todos os qubits, criando uma superposição uniforme de todos os estados possíveis da base computacional:

$$|s\rangle = H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$

Nesse estado, todos os elementos do espaço de busca possuem a mesma amplitude $1/\sqrt{N}$. Geometricamente, $|s\rangle$ pode ser decomposto em relação ao estado solução $|\omega\rangle$ e ao subespaço dos demais estados:

$$|s\rangle = \sin(\theta)|\omega\rangle + \cos(\theta)|s'\rangle$$

Onde θ é o ângulo que define a proximidade inicial entre o estado do sistema e a solução desejada.

2.2. O Oráculo Quântico (U_ω)

O oráculo identifica a solução aplicando uma inversão de fase apenas no estado $|\omega\rangle$:

$$U_\omega|x\rangle = \begin{cases} -|x\rangle & \text{se } x = \omega \\ |x\rangle & \text{se } x \neq \omega \end{cases}$$

Essa operação também pode ser expressa como:

$$U_\omega = I - 2|\omega\rangle\langle\omega|$$

Assim, o estado solução é marcado por uma inversão de fase, permitindo que as etapas seguintes ampliem sua probabilidade.

2.3. Operador de Difusão e Inversão pela Média (U_s)

Após a ação do oráculo, aplica-se o operador de difusão, responsável pela amplificação da amplitude da solução:

$$U_s = 2|s\rangle\langle s| - I$$

A combinação $G = U_s U_\omega$ define a Iteração de Grover, que pode ser interpretada geometricamente como uma rotação no plano formado por $|\omega\rangle$ e $|s'\rangle$, aumentando progressivamente a amplitude da solução.

Para um espaço de busca de tamanho N, o número ideal de iterações é:

$$k \approx \frac{\pi}{4}\sqrt{N}$$

Após aproximadamente k iterações, a medição do sistema retorna o estado $|\omega\rangle$ com alta probabilidade [Nielsen and Chuang 2010].

3. Metodologia e Análise de Complexidade

Nesta seção, são descritos o fluxo de implementação do algoritmo e a análise quantitativa de seu desempenho em comparação ao modelo clássico.

3.1. Arquitetura do Circuito Quântico

A implementação do Algoritmo de Grover, proposta via IBM Qiskit, segue uma arquitetura lógica dividida em etapas. O circuito é composto pela inicialização com portas Hadamard (H), seguida pelo Oráculo e pelo operador de difusão (amplificação) [Grover 1996]. Conforme a lógica do projeto:

- **Inicialização**: Todos os qubits são colocados em superposição uniforme.
- **Oráculo**: Implementa-se a função lógica que inverte a fase do estado de interesse.
- **Amplificação**:Aplica-se a sequência de portas H, X e Z controladas para realizar a inversão pela média.

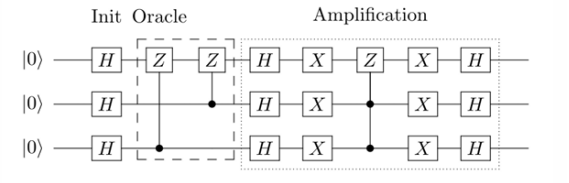

Figura 1. Esquema padrão do circuito quântico (Arquitetura Lógica).

A repetição desses blocos (Oráculo e Amplificador) mostrado na figura 1, é o que garante que o vetor de estado seja rotacionado gradualmente até o acerto.

3.2. Análise da Complexidade (Big O)

A eficiência do Algoritmo de Grover é medida pelo número de consultas ao oráculo necessárias para encontrar o estado-alvo com alta probabilidade. Em um computador clássico, a busca em um espaço não ordenado de tamanho N requer, em média, $N/2$ consultas, resultando em complexidade $O(N)$.

No modelo quântico, a solução pode ser encontrada com aproximadamente $\frac{\pi}{4}\sqrt{N}$ operações, caracterizando uma aceleração quadrática. A Figura 2 apresenta a comparação entre as complexidades.

É notado que, à medida que o espaço de busca (N) cresce, a vantagem quântica torna-se cada vez mais significativa, reduzindo o número de operações necessárias em comparação com a busca clássica.

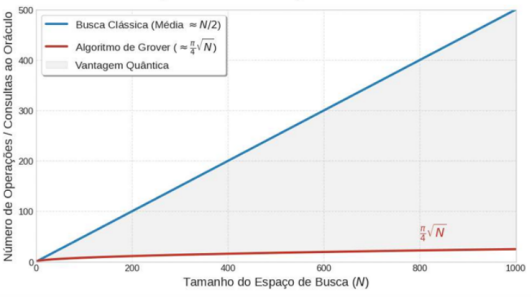

Figura 2. Complexidade Exata: Força Bruta vs. Grover.

4. Resultados Esperados e Discussão

A análise do Algoritmo de Grover revela impactos diretos na segurança atual. Com base na aceleração quadrática discutida, os resultados esperados deste estudo apontam que:

- **Vulnerabilidade do AES-128:** Devido à redução da complexidade de busca para $\sqrt{2^{128}} = 2^{64}$, o padrão AES-128 deixa de oferecer o nível de segurança de 128 bits, tornando-se vulnerável a ataques de força bruta realizados por computadores quânticos de larga escala.
- **Redução da Eficácia:** O algoritmo de Grover reduz a segurança efetiva da chave pela metade, embora não quebre a criptografia simétrica de forma instantânea como o Algoritmo de Shor faz com a criptografia assimétrica.
- **Resistência do AES-256:** O padrão AES-256 mantém uma margem de segurança de 128 bits sob ataque quântico ($\sqrt{2^{256}} = 2^{128}$), sendo a alternativa recomendada para garantir a confidencialidade na era pós-quântica [Stallings 2017].

5. Conclusão

Este trabalho demonstrou que a computação quântica, por meio do Algoritmo de Grover, altera o risco em sistemas criptográficos simétricos. A transição da busca clássica linear para a busca quântica quadrática exige que administradores de sistemas e desenvolvedores adotem medidas preventivas imediatas, especialmente a duplicação do tamanho das chaves. Como trabalhos futuros, pretende-se realizar a implementação prática de circuitos simplificados no IBM Qiskit para validar o aumento da probabilidade de acerto conforme o aumento do número do operador de difusão [Abbas et al. 2020].

Referências

Abbas, A. et al. (2020). Learn quantum computation using qiskit. IBM. Disponível em: `http://qiskit.org/textbook`. Acesso em: nov. 2025.

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. In *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, pages 212–219.

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

Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice*. Pearson, 7th edition.