VIII Simpósio de Iniciação Científica 2025

"Do conhecimento acadêmico à transformação sustentável: inovação com validação científica"

COMPUTAÇÃO QUÂNTICA APLICADA À HARDWARE CONFIGURÁVEL COM FOCO EM SEGURANÇA DA INFORMAÇÃO

Gustavo Inácio Arraes Fernandes (IC), Otávio de Souza Martins Gomes (PQ)[1]
[1]*Universidade Federal de Itajubá*

Palavras-chave: Algoritmos quânticos. Criptografia pós-quântica. FPGA. Grover. Segurança da Informação.

Introdução

A segurança da informação enfrenta mudanças significativas diante do avanço da computação quântica, que representa uma ameaça concreta aos sistemas criptográficos clássicos. Algoritmos quânticos podem reduzir a complexidade de ataques de força bruta e de pré-imagem contra cifras e funções de hash. Um exemplo é o Algoritmo de Grover, que acelera buscas em bases não ordenadas. Por isso, chaves simétricas como as do padrão AES-128 perdem parte de sua robustez: uma busca exaustiva em 2^{128} possibilidades é reduzida a apenas 2^{64} tentativas. Esse impacto é particularmente grave na criptografia simétrica e em funções hash, como discutido por Bernstein e Lange (2017) e Alagic et al. (2022).

Esse cenário evidencia a urgência na avaliação prática de algoritmos quânticos, tanto ofensivos quanto defensivos, como forma de compreender de maneira realista seus impactos na cibersegurança. Entretanto, o acesso a computadores quânticos reais permanece restrito, de alto custo e grande complexidade de operação. Como alternativa, sistemas clássicos têm sido utilizados na emulação de circuitos quânticos. Simuladores baseados em software, como o Qiskit (IBM Quantum, 2023), oferecem boa fidelidade matemática, mas encontram limitações quanto ao paralelismo intrínseco à computação quântica e à aplicação em sistemas embarcados ou de tempo real.

Para compreender os impactos da computação quântica, é importante introduzir alguns conceitos fundamentais. O qubit é a unidade básica de informação, capaz de assumir simultaneamente os estados $|0\rangle$ e $|1\rangle$ (Nielsen; Chuang, 2000) por meio do princípio da superposição. Quando múltiplos qubits interagem, ocorre o entrelaçamento, fenômeno em que o estado de um qubit não pode ser descrito independentemente dos demais. Essas propriedades permitem que algoritmos quânticos explorem o paralelismo intrínseco da mecânica quântica para acelerar tarefas específicas. O Algoritmo de Grover, em particular, utiliza iterações baseadas em um oráculo e um difusor para aumentar a probabilidade de encontrar rapidamente o estado procurado, reduzindo a complexidade de buscas em bancos de dados não estruturados.

O objetivo central desta pesquisa é implementar e validar uma arquitetura modular em FPGA para emulação do Algoritmo de Grover, através da criação de uma biblioteca com as portas lógicas fundamentais da computação quântica. Explora-se sua aplicabilidade em segurança da informação e destacando também seu potencial como ferramenta educacional e de prototipagem.

Para isso, propõe-se descrição de hardware em Verilog HDL, síntese e simulação utilizando Quartus Prime, representação da unidade de informação quântica (qubit) em aritmética de ponto fixo (Q1.14) para precisão e redução de consumo de recursos e integração com um microcontrolador via UART para monitoramento e validação dos resultados. A comparação com simulações matemáticas via Qiskit garante a fidelidade da emulação.

Assim, este trabalho oferece uma ferramenta acessível para estudo da segurança da informação em um cenário pós-quântico, fornecendo uma abordagem prática que garante o desenvolvimento futuro de novas soluções dada a sua natureza modular e escalável.

Metodologia

O sistema foi desenvolvido no ambiente Altera Quartus Prime Lite Edition 18.1, utilizado tanto para a síntese dos circuitos lógicos quanto para a integração com o simulador ModelSim, ferramenta que possibilitou monitoramento detalhado dos sinais em nível de ciclo de clock. A plataforma escolhida para a implementação foi a FPGA Altera MAX 10 (10M50DAF484C7G), que se destaca pelo equilíbrio entre custo e quantidade de recursos, sendo apropriada para aplicações de prototipagem em cenários de baixo consumo e tempo real.

Os circuitos foram descritos em Verilog HDL,

priorizando modularização, escalabilidade e compatibilidade com pipeline. Cada módulo lógico foi projetado para representar uma operação unitária específica, sendo interconectado no módulo principal (*emulator.v*). Essa estratégia permitiu a reutilização e adaptação de portas em diferentes cenários, além de facilitar a expansão para circuitos maiores.

A representação dos qubits foi realizada em aritmética de ponto fixo no formato Q1.14, totalizando 16 bits por componente. Esse formato dedica 1 bit ao sinal, 1 bit à parte inteira e 14 bits à parte fracionária, possibilitando representar números no intervalo aproximado de -2 a 1,999 com boa precisão. Essa escolha equilibra fidelidade matemática com baixo consumo de recursos lógicos, sendo adequada para operações unitárias comuns na computação quântica.

As portas lógicas quânticas foram emuladas a partir de suas representações matriciais, conforme o formalismo da mecânica quântica (Nielsen; Chuang, 2000), sendo adaptadas para operações aritméticas digitais. Constantes irracionais, como o fator $1/\sqrt{2}$ da porta Hadamard, foram implementadas diretamente em ponto fixo. Foi desenvolvido um módulo específico para representar qubits entrelaçados. Ele garante a sincronização correta entre os estados e permite emular o fenômeno do entrelaçamento, essencial para a execução de algoritmos como o de Grover.

Ao término da execução, os coeficientes atualizados de cada qubit são enviados ao módulo *uart_sender.v*, responsável por transmitir os dados via UART (Universal Asynchronous Receiver-Transmitter). Essa comunicação ocorre com um microcontrolador ESP32, que atua como interface de monitoramento e análise. O ESP32 permitiu comparar experimentalmente os resultados obtidos na FPGA com os gerados por simulações no Qiskit, assegurando a fidelidade da implementação.

A implementação do Algoritmo de Grover foi realizada exclusivamente com portas básicas (Hadamard, X, CNOT e Toffoli), em conjunto com o registrador de estados entrelaçados. Para validação prática, foi definido um espaço de busca com quatro estados $|00\rangle,|01\rangle,|10\rangle,|11\rangle$ sendo o estado alvo estabelecido em $|01\rangle$. Esse experimento possibilitou comprovar a viabilidade da arquitetura proposta e servir como base para futuros escalonamentos.

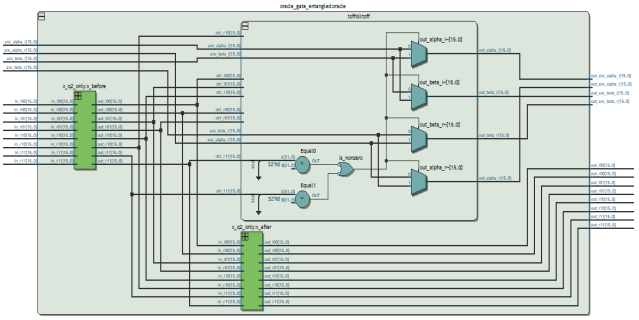

Figura 1 – Diagrama RTL do componente Oráculo. *(Fonte: Elaborado pelo autor, 2025).*

Resultados e discussão

A comparação entre os resultados obtidos na FPGA e as simulações no Qiskit demonstrou a fidelidade da emulação proposta. A análise de erro absoluto, definida pela diferença entre os coeficientes ideais e os discretizados em ponto fixo, indicou valores da ordem de $2{,}05\times10^{-5}$, compatíveis com o reportado na literatura (Khalid et al., 2004), que apresentou $3{,}05\times10^{-5}$, Esse resultado evidencia a precisão alcançada pela escolha do formato Q1.14, mesmo utilizando recursos lógicos significativamente inferiores.

A porta Hadamard apresentou maior sensibilidade a erros acumulados devido ao uso de constantes irracionais, enquanto as portas X, CNOT e Toffoli exibiram erros desprezíveis, reforçando a robustez da abordagem.

Tabela 1 – Erro absoluto na porta Hadamard.

Fonte	Erro Absoluto (E)
Khalid et al. (2004)	$3{,}05\times10^{-5}$
Este trabalho	$2{,}05\times10^{-5}$

Quanto ao uso de recursos, a implementação ocupou apenas 57 células lógicas (0,11%) e 38 registradores (0,07%), um contraste expressivo em relação a Khalid et al., cuja versão demandava 12.636 células lógicas em uma FPGA Stratix. Essa eficiência viabiliza o escalonamento do sistema para mais qubits sem comprometer a viabilidade prática.

Tabela 2 – Comparação do uso de recursos lógicos.

Fonte	LCs Utilizadas	Registradores
Khalid et al. (2004)	12.636	Não especificado
Este trabalho	57 (0,11%)	38 (0,07%)

A escolha de Khalid et al. (2004) como referência não está ligada à atualidade, mas à clareza metodológica. O trabalho apresenta uma implementação em FPGA com aritmética de ponto fixo, o que permite comparar de forma transparente erros absolutos e uso de recursos lógicos. Em contraste, estudos mais recentes focam em outros objetivos, como otimizações tensoriais e trigonômicas (Jungjarassub; Piromsopa, 2022) ou arquiteturas escaláveis de alto consumo de memória e paralelismo (Belfore II, 2024). Esses trabalhos visam simulação em larga escala, enquanto nossa proposta busca simplicidade e viabilidade em sistemas embarcados. Nesse sentido, Khalid et al. servem como benchmark adequado para avaliar os trade-offs entre desempenho e baixo custo, reforçando a relevância da arquitetura em aplicações práticas e educacionais.

O tempo de execução também foi avaliado. O algoritmo utilizou 12 ciclos de clock a 50 MHz, correspondendo a 240 ns. O tempo de execução foi de 240 ns, mais lento que os 84 ns de Khalid et al. Ainda assim, é 360 mil vezes mais rápido que a simulação no Qiskit (87,25 ms), reforçando a eficiência da abordagem.

Tabela 3 – Comparação de tempos de execução.

Plataforma	Tempo de execução
FPGA (Khalid et al.)	84 ns
FPGA (este trabalho)	240 ns
Qiskit (simulação)	87,25 ms

Além da validação funcional, a arquitetura mostrou-se promissora como ferramenta de análise e escalabilidade. A baixa ocupação de recursos lógicos permite a construção de oráculos mais complexos, como os presentes na cifra AES (Viamontes; Markov; Hayes, 2005). Dessa forma, torna-se possível medir o custo prático, em termos de tempo de execução e consumo de hardware, de ataques quânticos simulados, oferecendo uma estimativa realista do impacto desses algoritmos sobre protocolos criptográficos atuais.

Outro aspecto relevante é que, graças à modularidade do projeto, os oráculos podem ser adaptados para diferentes problemas e avaliados com precisão em nível de ciclo de clock. Isso possibilita mover a análise da complexidade teórica $O(\sqrt{2})$ para previsões temporais concretas em nanossegundos, ampliando o valor da plataforma não apenas para ensino, mas também para prototipação de cenários de ataque e defesa em segurança da informação.

Apesar dos resultados positivos, algumas limitações precisam ser reconhecidas para oferecer uma avaliação equilibrada da proposta. A principal delas diz respeito à escalabilidade: a implementação atual é adequada apenas para poucos qubits (2 a 3), e a expansão para circuitos maiores exigiria um crescimento exponencial no consumo de recursos de hardware, o que restringe sua aplicação em FPGAs de baixo porte.

Outro ponto está relacionado ao tempo de execução. Embora a arquitetura tenha alcançado 240 ns, ainda é mais lenta que a de Khalid et al. (84 ns). Essa diferença decorre da decisão de priorizar simplicidade e baixo custo, em detrimento do paralelismo máximo possível, reforçando o caráter da proposta como uma solução de baixo consumo e não de desempenho extremo.

Além disso, a representação de constantes irracionais em ponto fixo, como no caso da porta Hadamard, introduz erros acumulados que, embora pequenos no presente contexto, tendem a crescer em circuitos mais complexos. Por fim, a escolha de Khalid et al. como referência metodológica é adequada pela clareza e relevância técnica, mas não contempla os avanços mais recentes na área, que exploram escalabilidade massiva e arquiteturas de alto consumo de memória. Dessa forma, a proposta posiciona-se menos como alternativa competitiva a esses esforços e mais como uma ferramenta prática para ensino, análise embarcada e prototipagem em segurança da informação.

Conclusões

A pesquisa demonstrou a viabilidade do uso de FPGAs como plataforma de emulação de algoritmos quânticos, oferecendo baixo custo, simplicidade arquitetural e possibilidade de operação em tempo real.

A implementação do Algoritmo de Grover

evidenciou:

- Alta precisão, com erro absoluto da ordem de 10^{-5};
- Baixo consumo de recursos lógicos, utilizando apenas 57 células lógicas e 38 registradores;
- Desempenho satisfatório, com execução em 240 ns, milhares de vezes mais rápido que simulações em software.

Esses resultados confirmam a adequação da arquitetura não apenas como ferramenta de ensino e prototipagem, mas também como plataforma de análise prática de vulnerabilidades criptográficas em um cenário pós-quântico. O trabalho evidencia que o uso de hardware reconfigurável pode auxiliar na quantificação realista dos custos de ataques quânticos, contribuindo para o desenvolvimento de estratégias de defesa e mitigação em segurança da informação.

Como trabalhos futuros, pretende-se ampliar a biblioteca de portas quânticas e implementar algoritmos mais avançados, como os de Shor e Simon, avaliando o impacto de oráculos complexos, como os presentes em cifras reais (ex.: S-Box do AES). Além disso, busca-se integrar a plataforma a sistemas de distribuição de chaves quânticas (QKD), explorando sua utilização em cenários práticos de comunicação segura (Zhang et al., 2012). Essa evolução permitirá validar empiricamente a resiliência de protocolos pós-quânticos frente a ataques baseados em Grover e estabelecer um ambiente de prototipagem de novas técnicas de criptografia híbrida resistentes à computação quântica.

Assim, a arquitetura proposta não se limita a reproduzir algoritmos quânticos, mas também se consolida como instrumento de experimentação e análise de cibersegurança, capaz de apoiar tanto a pesquisa acadêmica quanto aplicações reais em sistemas embarcados.

Agradecimentos

O autor expressa sua gratidão à Universidade Federal de Itajubá (UNIFEI), ao Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), à Financiadora de Estudos e Projetos (FINEP) e ao projeto Clavis PlatCiber pelo apoio que tornaram este projeto possível.

Referências

NIELSEN, M. A.; CHUANG, I. L. *Quantum Computation and Quantum Information*. Cambridge: Cambridge University Press, 2000.

IBM QUANTUM. *Qiskit Documentation*. 2023. Disponível em: https://www.ibm.com/quantum/qiskit. Acesso em: 20 ago. 2025.

KHALID, A. U.; ZILIC, Z.; RADECKA, K. FPGA emulation of quantum circuits. In: *IEEE International Conference on Computer Design (ICCD)*, 2004. Anais [...]. [S. l.: s. n.], 2004.

GROVER, L. K. A fast quantum mechanical algorithm for database search. In: *Annual ACM Symposium on Theory of Computing*, 28., 1996, Philadelphia. Proceedings [...]. New York: ACM, 1996. p. 212–219.

BERNSTEIN, D. J.; LANGE, T. Post-quantum cryptography. *Nature*, London, v. 549, p. 188–194, 2017. DOI: 10.1038/nature23461.

ALAGIC, G. et al. *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process*. Gaithersburg: NIST, 2022. (NISTIR 8413). Disponível em: https://doi.org/10.6028/NIST.IR.8413. Acesso em: 20 ago. 2025.

ZHANG, H. et al. A real-time QKD system based on FPGA. *Journal of Lightwave Technology*, v. 30, n. 18, p. 3026–3030, 2012. DOI: 10.1109/JLT.2012.2207938.

VIAMONTES, G. F.; MARKOV, I. L.; HAYES, J. P. Is quantum search practical? *Computing in Science & Engineering*, v. 7, n. 3, p. 22–30, 2005. DOI: 10.1109/MCSE.2005.53.

BELFORE II, L. A. A scalable FPGA architecture for quantum computing simulation. *arXiv*, 2024. Disponível em: https://doi.org/10.48550/arXiv.2407.06415. Acesso em: 20 ago. 2025.

JUNGJARASSUB, Y.; PIROMSOPA, K. A performance optimization of quantum computing simulation using FPGA. In: *INTERNATIONAL CONFERENCE ON ELECTRICAL ENGINEERING/ELECTRONICS, COMPUTER, TELECOMMUNICATIONS AND INFORMATION TECHNOLOGY (ECTI-CON)*, 19., 2022, [S. l.]. Proceedings [...]. [S. l.: s. n.], 2022. DOI: 10.1109/ECTI-CON54298.2022.9795495.