# Análise experimental da ameaça quântica à criptografia clássica pelo Algoritmo de Shor em simuladores ideais vs. hardware real na Arquitetura Heron

**Luis Lima**[1], **Rosiane freitas** [2]

[1] Instituto de Computação – Universidade Federal do Amazonas (IComp/UFAM)
Manaus – AM, Brasil
{luis.lima, rosiane}@icomp.ufam.edu.br

***Abstract.*** *Shor's algorithm threatens asymmetric cryptography (RSA, ECC), but NISQ era constraints such as noise and decoherence hinder its practical execution. This paper empirically evaluates Shor's algorithm on the IBM Heron processor (`ibm_fez`), contrasting theoretical scaling with physical feasibility. For $N = 55$, the standard architecture ($m = 2L$) generated over 96,667 CNOT gates, degrading the quantum signal to statistical noise . To mitigate this, we evaluate an optimized architecture by reducing the measurement register to $m = L$, achieving a $\approx 49\%$ reduction in entangling gates and preserving discernible peaks under thermal noise. We conclude that strict technological barriers delay the immediate physical threat, providing a factual baseline for managing post-quantum cryptography (PQC) timelines without alarmism.*
***Keywords:*** *asymmetric cryptography, CNOT entanglement gates, NISQ era, post-quantum cryptography (PQC), quantum threat, Shor's quantum algorithm.*

***Resumo.*** *O algoritmo de Shor ameaça a criptografia assimétrica (RSA, ECC), mas restrições da era NISQ como ruído e decoerência limitam sua execução prática. Neste artigo é avaliado empiricamente o algoritmo de Shor no processador IBM Heron (`ibm_fez`), contrastando a complexidade teórica com a viabilidade física. Para $N = 55$ (número a fatorar, com $L = 6$ bits), a arquitetura padrão com registrador de medição $m = 2L$ gerou mais de 96,667 portas CNOT, degradando o sinal para ruído estatístico. Como mitigação, avaliou-se uma arquitetura otimizada com $m = L$, o que reduziu as portas de emaranhamento em $\approx 49\%$ e preservou picos discerníveis sob ruído térmico. Conclui-se que barreiras tecnológicas rigorosas limitam a ameaça imediata, oferecendo uma base factual para o planejamento da migração pós-quântica (PQC) com urgência mas sem alarmismos.*
***Palavras-chave:*** *ameaça quântica, algoritmo quântico de Shor, criptografia assimétrica, criptografia pós-quântica (PQC), era NISQ, portas de emaranhamento.*

## 1. Introdução

A computação quântica altera radicalmente o processamento de dados, superando limitações clássicas em problemas complexos como a fatoração de números inteiros, base da criptografia de chave pública atual. Enquanto a segurança contemporânea repousa na intratabilidade de algoritmos clássicos como o *General Number Field Sieve* (GNFS), o

algoritmo de Shor rompe este paradigma ao oferecer aceleração exponencial com complexidade polinomial $\mathcal{O}(n^3)$, ameaçando diretamente protocolos como o RSA.

Contudo, a materialização dessa ameaça enfrenta os limites da atual era NISQ (*Noisy Intermediate-Scale Quantum*). Ruído térmico, decoerência e a baixa fidelidade de portas lógicas em especial as portas CNOT (*Controlled-NOT*) restringem severamente a profundidade dos circuitos e degradam o estado quântico antes da medição.

Para mitigar essas limitações, em consonância com os esforços de execução compilada e otimizada de circuitos do algoritmo de Shor explorados pioneiramente por Amico et al. [Amico et al. 2019] e Skosana e Tame [Skosana and Tame 2022] para instâncias reduzidas, este trabalho investiga o equilíbrio entre a precisão teórica e a viabilidade física em hardware de última geração. Propõe-se uma análise comparativa extensiva entre a arquitetura padrão de Shor ($m = 2L$) e a configuração otimizada de precisão reduzida ($m = L$). A metodologia utiliza o simulador PennyLane para o cenário ideal e o processador `ibm_fez` (arquitetura IBM Heron) para validação física nas instâncias $N \in \{15, 21, 33, 35, 55\}$ expandindo o escopo das investigações anteriores [Amico et al. 2019, Skosana and Tame 2022], mapeando rigorosamente os pontos de ruptura do hardware moderno por meio de métricas quantitativas de fidelidade.

## 2. Fundamentação Teórica

A **computação quântica** utiliza o ***qubit*** como unidade básica de informação. Diferente do bit clássico, o qubit explora a ***superposição*** e o ***emaranhamento***, fenômenos físicos essenciais para a aceleração algorítmica [Nielsen and Chuang 2010]. Manipulados por portas lógicas, esses estados baseiam técnicas como a ***Transformada Quântica de Fourier*** (QFT), que fundamenta o algoritmo de Shor [Shor 1994].

### 2.1. Evolução e Estado-da-Arte em Hardware Quântico

Após os marcos teóricos fundamentais, a validação experimental de componentes físicos impulsionou a busca pela escalabilidade do modelo universal. Atualmente, o **estado-da-arte** transita da era NISQ (*Noisy Intermediate-Scale Quantum*) para os estágios iniciais de tolerância a falhas, onde a literatura prioriza o desenvolvimento de **qubits lógicos** (com correção de erros) em vez do simples aumento bruto de qubits físicos. As principais arquiteturas físicas em desenvolvimento incluem:

- **Qubits supercondutores:** Destacam-se pela velocidade de operação e são o foco dos principais roteiros de escalabilidade industrial, embora enfrentem severos desafios físicos relacionados à coerência térmica e ao ruído de diafonia (*crosstalk*).
- **Íons aprisionados:** Apresentam altíssimas taxas de fidelidade e tempos de coerência prolongados, sendo limitados primariamente pela velocidade de operação e pelos desafios de escalabilidade no confinamento a laser.
- **Átomos neutros e fótons:** Plataformas exploradas por sua alta conectividade topológica natural e potencial de operação contínua em temperatura ambiente.

### 2.2. Ameaça Quântica e Transição Criptográfica

No contexto da segurança da informação, a **ameaça quântica** centra-se na capacidade de algoritmos executados em computadores quânticos quebrarem os esquemas de criptografia assimétrica vigentes (como RSA e ECC). Avanços recentes na literatura de estimativa

de recursos demonstram que a fatoração de um inteiro RSA de 2048 bits pode ser realizada em menos de uma semana utilizando menos de um milhão de qubits físicos ruidosos, demandando configurações na ordem de 1.399 qubits lógicos sob códigos de correção de erros [Gidney 2025].

Essa viabilidade de quebra em tempo útil agrava a tática adversarial conhecida como ***harvest now, decrypt later*** (HNDL), na qual dados criptografados que trafegam atualmente são interceptados e armazenados para decriptografia futura [Dubey and Varshney 2026, Zelenovic et al. 2026]. Medições em larga escala na infraestrutura da internet revelam que, embora mecanismos híbridos pós-quânticos de troca de chaves comecem a ser adotados, a imensa maioria da autenticação via certificados TLS permanece baseada em assinaturas clássicas, mantendo os sistemas criticamente vulneráveis a ataques de falsificação no longo prazo [Dubey and Varshney 2026].

Diante desse cenário, a transição para a Criptografia Pós-Quântica (PQC) demanda abordagens de governança estruturadas, como a implementação de Registros de Exposição Quântica (QER), que priorizam a migração de ativos com base no tempo de vida exigido para a confidencialidade dos dados (*confidentiality horizon*) e nas restrições de infraestrutura [Zelenovic et al. 2026].

Por fim, a adoção iminente de esquemas PQC introduz severos desafios de desempenho. A substituição por padrões resistentes a ataques quânticos exige assinaturas e chaves substancialmente maiores. Em ambientes com recursos restritos (como IoT e sistemas embarcados), essa sobrecarga aumenta drasticamente o tempo de *handshake* e o consumo energético [Rassekhnia 2026]. Da mesma forma, em arquiteturas descentralizadas, o aumento no tamanho das transações reduz a vazão teórica e acelera o inchaço dos ledgers, exigindo adaptações profundas nos protocolos de consenso [Mallick et al. 2025].

## 3. O Problema da Fatoração e a Ameaça à Criptografia Assimétrica

O algoritmo de Shor [Shor 1994] representa uma ameaça catastrófica à criptografia assimétrica por resolver os problemas de fatoração de inteiros e logaritmo discreto em tempo polinomial. Diferentemente do algoritmo de Grover, que impõe uma aceleração quadrática mitigável pelo aumento de chaves, Shor torna obsoletos esquemas como o RSA, baseados na suposta intratabilidade clássica da decomposição de um composto $N = p \times q$.

Seja $N$ um inteiro de $n$ bits, o objetivo clássico é encontrar um fator não trivial $d$ ($1 < d < N$). O método clássico mais eficiente para chaves comerciais é o ***General Number Field Sieve*** **(GNFS)** [Lenstra and Lenstra 1993]. Superando abordagens determinísticas como o Crivo de Eratóstenes, o GNFS utiliza uma abordagem subexponencial de "congruência de quadrados", buscando relações da forma $x^2 \equiv y^2 \pmod{N}$, o que implica que $(x - y)(x + y) = kN$. A partir disso, extrai-se um fator não trivial de $N$ via Máximo Divisor Comum, $\gcd(x - y, N)$. A complexidade assintótica do GNFS é subexponencial [Lenstra and Lenstra 1993], tornando-se impraticável para o RSA-2048.

**Algoritmo de Shor:** Shor resolve a fatoração de $N$ ao reduzi-la à busca do período $r$ de uma função de exponenciação modular $f(x) = a^x \pmod{N}$. A arquitetura utiliza dois registradores: o primeiro com $t$ qubits para consulta ($2^t \approx N^2$) e o segundo com $n$ qubits para armazenar os valores da função.

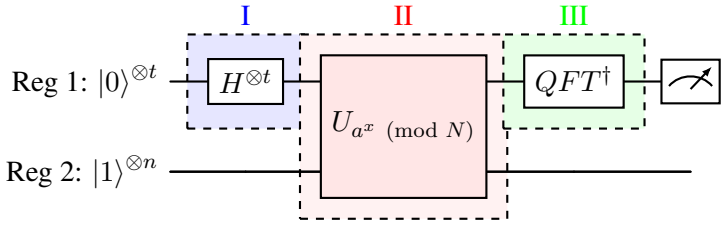


**Figura 1. Circuito genérico de Shor baseado em [Nielsen and Chuang 2010]: I (Superposição), II (Exponenciação Modular) e III (QFT Inversa).**

**Etapa I: Superposição**
A aplicação de portas Hadamard gera:

$$|\Psi_1\rangle = \frac{1}{\sqrt{2^t}} \sum_{x=0}^{2^t-1} |x\rangle\, |0\rangle^{\otimes n}$$

**Etapa II: Oráculo Quântico**
O operador $U_{a,N}$ codifica o período $r$ na função modular:

$$|\Psi_2\rangle = \frac{1}{\sqrt{2^t}} \sum_{x=0}^{2^t-1} |x\rangle\, |a^x \pmod N\rangle$$

**Etapa III: QFT Inversa**
A $QFT^\dagger$ é aplicada ao primeiro registrador para extrair a fase:

$$|\Psi_3\rangle = \frac{1}{2^t} \sum_{y=0}^{2^t-1} \sum_{x=0}^{2^t-1} e^{-\frac{2\pi i x y}{2^t}} |y\rangle\, |f(x)\rangle$$

**Pós-processamento:**
Após a medição de $y$, utiliza-se frações contínuas para obter $r$, tal que:

$$\text{fator} = \gcd(a^{r/2} \pm 1, N)$$

A viabilidade prática deste algoritmo depende da correção de erros quânticos, mas a prova teórica de Shor estabeleceu a base para a necessidade da Criptografia Pós-Quântica (PQC). A fatoração de inteiros sustenta a criptografia RSA. A Figura 2 demonstra como o algoritmo de Shor transforma um problema intratável em tratável.

**GNFS**

**function** GNFS($n$)
  Escolher $f, m$
  Construir bases
  **for** $(a, b)$ coprimos **do**
    **if** suaves **then** Guardar
    **end if**
  **end for**
  Matriz $M$ e achar $\mathbf{v}$
  $x^2 \equiv y^2 \pmod n$
  $g \leftarrow$ MDC$(x - y, n)$
  **return** $g$
**end function**

**Shor Classico**

**function** SHORCLASS($n$)
  Escolher $a$
  **if** MDC $> 1$ **then return**
  **end if**
  $r \leftarrow 1$
  **while** $a^r \pmod n \neq 1$ **do**
    $r \leftarrow r + 1$
  **end while**
  **if** $r$ par e $a^{r/2} \neq n - 1$ **then**
    **return** $f, n/f$
  **end if**
**end function**

**Shor quântico**

**function** ENCONTRARPQ($n, a$)
  $t \leftarrow 2nn$
  Regs $\leftarrow |0\rangle$
  Aplicar $H^{\otimes t}$
  Aplicar $U_{a,n}$
  Aplicar QFT$^\dagger$
  $m \leftarrow$ Medir
  $r \leftarrow$ FraçõesCont.
  **return** $r$
**end function**

**Figura 2. Comparação de paradigmas para fatoração.**

O algoritmo clássico **GNFS**(esquerda) opera através da coleta massiva de relações numéricas (etapa de Peneira) e resolução de sistemas lineares, resultando em complexidade super-polinomial.

A inovação de Shor foi reduzir o problema da fatoração ao problema de encontrar o período $r$ de uma função (centro). Classicamente, encontrar esse período é tão difícil quanto fatorar (custo exponencial). A **Sub-rotina Quântica(direita)** resolve este gargalo específico. Utilizando a Transformada de Fourier Quântica Inversa (QFT$^\dagger$), o algoritmo consegue interferir destrutivamente todas as frequências incorretas e construtivamente a frequência do período $r$, permitindo sua determinação em tempo polinomial.

**Tabela 1. Comparação de Complexidade do Problema de Fatoração**

| Algoritmo | Complexidade de Tempo | Tipo de Crescimento |
|---|---|---|
| GNFS (Clássico) | $O\left(e^{c \cdot n^{1/3} (\log n)^{2/3}}\right)$ | Sub-exponencial |
| Shor Clássico | $O(2^{n/3})$ | Exponencial |
| Shor Quântico | $O(n^3)$ | Polinomial |

Nota: $n$ representa o número de bits do inteiro $N$.

A análise comparativa da Tabela 1 evidencia o abismo entre os paradigmas. Enquanto o GNFS possui complexidade sub-exponencial tornando a fatoração de chaves RSA-2048 impraticável para supercomputadores clássicos o algoritmo de Shor atinge complexidade polinomial $O(n^3)$. Ao resolver o gargalo da busca pelo período $r$ via interferência quântica, Shor transforma a fatoração em um problema tratável, condicionado apenas à escala do hardware. Essa quebra de paradigma justifica a transição urgente para a Criptografia Pós-Quântica (PQC).

### 3.1. Ameaça do Shor aos Sistemas Criptográficos Assimétricos

O algoritmo de Shor compromete fundamentalmente todos os esquemas criptográficos baseados na dificuldade de fatoração e logaritmo discreto.

#### 3.1.1. RSA (*Rivest-Shamir-Adleman*)

O RSA, amplamente utilizado em comunicações seguras, assinaturas digitais e protocolos TLS/SSL, baseia sua segurança na dificuldade de fatorar o módulo $N = p \times q$. Com o Algoritmo de Shor, um adversário quântico pode:

1. Obter a chave pública $(N, e)$ do destinatário;
2. Executar o algoritmo de Shor para fatorar $N$ e recuperar $p$ e $q$;
3. Calcular $\phi(N) = (p-1)(q-1)$;
4. Calcular a chave privada $d \equiv e^{-1} \pmod{\phi(N)}$;
5. Decifrar todas as mensagens cifradas com a chave pública comprometida.

#### 3.1.2. ECC (*Elliptic Curve Cryptography*)

A criptografia de curvas elípticas (ECC) baseia sua segurança no problema do logaritmo discreto em curvas elípticas. A versão do algoritmo de Shor para logaritmo discreto resolve este problema em tempo polinomial, comprometendo completamente esquemas como:

- ECDH (Elliptic Curve Diffie-Hellman) para estabelecimento de chaves;
- ECDSA (Elliptic Curve Digital Signature Algorithm) para assinaturas digitais;
- Curvas como secp256k1 (utilizada em Bitcoin e blockchain) e Curve25519.

#### 3.1.3. Outros Esquemas Criptográficos Assimétricos Ameaçados

- **Diffie-Hellman**: estabelecimento de chaves em TLS, VPNs, SSH;
- **DSA (Digital Signature Algorithm)**: assinaturas digitais;
- **ElGamal**: criptografia e assinaturas;
- **Algoritmos baseados em pareamento**: criptografia baseada em identidades.

Um resumo dos principais esquemas afetados e suas respectivas aplicações pode ser visualizado na Tabela 2.

**Tabela 2. Esquemas criptográficos afetados pelo algoritmo de Shor**

| Esquema | Prob. Matemático | Aplicação Principal |
|---|---|---|
| RSA | Fatoração de inteiros | TLS, SSH, Assinaturas, E-mail |
| ECDSA | Log. discreto (ECC) | Assinaturas, Blockchain |
| ECDH | Log. discreto (ECC) | Acordo de chaves |
| Diffie-Hellman | Log. discreto | TLS, VPNs, IPsec |
| DSA | Log. discreto | Assinaturas |
| ElGamal | Log. discreto | Criptografia e Assinaturas |

### 3.2. Migração para Criptografia Pós-Quântica

Diferentemente do cenário simétrico, onde o aumento de parâmetros mitiga a ameaça de Grover, a criptografia assimétrica **exige a substituição completa** dos esquemas comprometidos por alternativas resistentes a ataques quânticos.

#### 3.2.1. Padrões do NIST

O NIST finalizou em 2024 os primeiros padrões de criptografia pós-quântica (PQC) [National Institute of Standards and Technology 2024], conforme listado na Tabela 3:

**Tabela 3. Padrões de Criptografia Pós-Quântica do NIST**

| Padrão | Algoritmo | Finalidade |
|---|---|---|
| FIPS 203 | ML-KEM (Kyber) | Cripto. geral (KEM) |
| FIPS 204 | ML-DSA (Dilithium) | Assinatura digital |
| FIPS 205 | SLH-DSA (SPHINCS+) | Assinatura (backup) |
| – | HQC | Cripto. alternativa |

#### 3.2.2. Desafios da Migração

A transição para criptografia pós-quântica apresenta desafios significativos: (1) **Tamanho de chaves e assinaturas**: algoritmos PQC geralmente possuem chaves e assinaturas significativamente maiores que os equivalentes clássicos, como detalhado na Tabela 4; (2) **Performance**: operações criptográficas podem ser mais custosas computacionalmente; (3) **Interoperabilidade**: sistemas legados precisam ser atualizados ou substituídos; (4) **Crypto-agility**: capacidade de sistemas substituírem algoritmos criptográficos rapidamente torna-se requisito arquitetônico essencial.

**Tabela 4. Comparação entre RSA e ML-KEM (Kyber)**

| Esquema | Chave púb. | Chave priv. | Cifrado |
|---|---|---|---|
| RSA-2048 | 256 bytes | 1.2 KB | 256 bytes |
| ML-KEM-768 | 1.184 bytes | 2.400 bytes | 1.088 bytes |

## 4. O Abismo NISQ: Limitações de Hardware Real

Nesta seção, analisa-se o impacto das restrições físicas dos processadores da era NISQ (*Noisy Intermediate-Scale Quantum*) na execução do algoritmo de Shor. Confronta-se a elegância da complexidade teórica com as barreiras práticas de ruído e hardware, evidenciando o fosso existente entre os modelos ideais e a realidade experimental.

### 4.1. Decoerência e Limitações da Supercondutividade

A computação quântica contemporânea enfrenta severas limitações devido à extrema sensibilidade dos sistemas ao ambiente. No contexto do processador IBM Heron (ibm_fez), os qubits baseiam-se em circuitos de **supercondutividade**, que, embora ofereçam alta velocidade de operação, sofrem drasticamente com instabilidades térmicas e ruído de diafonia (*crosstalk*). O fenômeno da **decoerência quântica** [Nielsen and Chuang 2010] descreve a perda dessa informação para o meio, destruindo os estados de superposição e emaranhamento vitais para a aceleração algorítmica.

Fisicamente, essa restrição é ditada por duas métricas temporais essenciais:

- **Tempo de Relaxação Térmica ($T_1$):** Intervalo médio para o qubit decair do estado excitado ($|1\rangle$) para o fundamental ($|0\rangle$);
- **Tempo de Desfocagem Quântica ($T_2$):** Limiar em que o qubit perde sua relação de fase, transformando a superposição coerente em uma mistura clássica.

Como o algoritmo de Shor [Shor 1994] exige operações modulares sequenciais massivas, a preservação do estado supercondutor torna-se o principal gargalo; se o tempo de execução do circuito ultrapassar os limites de $T_1$ e $T_2$, os qubits sofrem colapso prematuro. O resultado deixa de ser uma distribuição matemática válida e degrada-se irreversivelmente em ruído térmico.

### 4.2. Fidelidade de Portas e o Gargalo das CNOTs

No algoritmo de Shor, o oráculo de exponenciação modular [Nielsen and Chuang 2010] gera uma quantidade massiva de portas **CNOT** (*Controlled-NOT*), cuja taxa de erro é ordens de grandeza superior às de um qubit. Sem Correção de Erros Quânticos (QEC) ativa na era NISQ, a probabilidade de sucesso decai exponencialmente com o acúmulo de falhas, impondo um teto físico rígido à profundidade máxima do processador.

Essa barreira é evidenciada em tentativas históricas de fatorar instâncias mínimas (como $N = 15$ e 21). Ao cruzar a tolerância física do chip, a execução em hardware real diverge das simulações ideais e a interferência quântica construtiva que apontaria o período correto segundo Lenstra e Lenstra (1993) e Pomerance (1996) é totalmente obliterada. O resultado degrada-se em uma distribuição probabilística uniforme (**ruído branco**), derrubando a taxa de sucesso para patamares inferiores a $5\%$.

## 5. Trabalhos Relacionados

A viabilidade do algoritmo de Shor em hardwares NISQ confronta a vantagem teórica de sua escalabilidade polinomial $O(n^3)$ contra a complexidade subexponencial do método clássico *General Number Field Sieve* (GNFS) [Kavitha et al. 2025] com severas restrições físicas. Estima-se que seriam necessários 20 milhões de qubits ruidosos sob códigos de superfície para quebrar chaves comerciais RSA-2048 [Gidney and Ekerå 2021].

Nesse panorama de validação empírica, estudos pioneiros como o de [Amico et al. 2019] documentaram a execução compilada do algoritmo de Shor em chips IBM Q para instâncias de $N \in \{15, 21, 35\}$, enquanto [Skosana and Tame 2022] avançaram na otimização de portas lógicas (empregando variantes de fase relativa) para fatorar $N = 21$ em arquiteturas supercondutoras como o *Casablanca* e o *Toronto*. Tais investigações evidenciaram

que a engenharia e a compilação restrita de circuitos são indispensáveis para extrair sinal útil em meio às restrições do hardware.

O ruído acumulado e a decoerência continuam limitando severamente os dispositivos reais: experimentos de [Abdel-Rehim 2025] demonstram que, enquanto simulações ideais alcançam $N = 299$, o ruído físico reduz drasticamente esse teto devido ao erro proibitivo de portas CNOT. Adicionalmente, execuções em nuvem exigem construções sob medida para a topologia de cada chip [Bagourd et al. 2026].

Como mitigação, abordagens *Early Fault-Tolerant* focam na robustez contra despolarização em circuitos baseados em QFT [Dutkiewicz et al. 2025], enquanto cho2024 apontam que a eficiência na exponenciação modular e a redução de portas T são críticas na era NISQ. Nesse cenário, a redução do registro de contagem para $m = L$ fundamenta-se também na *Quantum Punctured Phase Estimation* [Lee et al. 2025], simplificando o circuito.

Pesquisas recentes também propõem QFT de profundidade logarítmica sem qubits auxiliares [Kahanamoku-Meyer et al. 2025], reúso de qubits em circuitos dinâmicos [Su et al. 2026] e substituição de unitárias controladas por não controladas para mitigar CNOTs [Amico 2026]. Na validação, emuladores como o UNIQUE reduzem expressivamente o tempo de simulação de operações aritméticas [Robertson and Ventura 2024]. Enquanto a literatura anterior concentrou-se majoritariamente em instâncias menores ($N \leq 35$) em gerações passadas de hardware [Amico et al. 2019, Skosana and Tame 2022], este trabalho avança o estado da arte ao avaliar a arquitetura otimizada ($m = L$) aplicada a instâncias escaladas até $N = 55$ diretamente no processador de última geração **IBM Heron** (`ibm_fez`), quantificando os limites empíricos de fidelidade e ruptura no hardware moderno.

## 6. Estudo de Caso: O Algoritmo de Shor no Processador IBM Heron

Para avaliar empiricamente o comportamento dos circuitos quânticos sob as restrições da era NISQ, realizou-se um estudo de caso prático aplicando o algoritmo de Shor para a fatoração de números semiprimos no hardware quântico real da IBM.

### 6.1. Definição de Fatores e Níveis

O plano experimental foi estruturado como um experimento fatorial completo, garantindo que todas as combinações de configurações de circuitos e instâncias numéricas fossem testadas sob as mesmas condições operacionais. Os fatores analíticos e seus respectivos níveis são definidos a seguir:

- **Fator 1: Arquitetura do Circuito Quântico ($A$):** Determina a dimensão do registrador de medição alocado para a transformada de Fourier quântica / Estimativa de Fase Quântica (QPE).
  - **Nível $A_1$ (Padrão):** Utiliza a especificação teórica canônica recomendada pela literatura ($m = 2L$ qubits), assegurando precisão matemática máxima no limite assintótico ideal.
  - **Nível $A_2$ (Otimizado / $m = L$):** Reduz o registrador de medição pela metade, gerando um circuito de menor profundidade e mitigando a taxa de erro combinatória induzida pelo ruído do sistema.

- **Fator 2: Instância do Problema ($N$):** O número inteiro semiprimo a ser fatorado pelo algoritmo. Foram selecionados cinco valores com níveis crescentes de complexidade algébrica: $N \in \{15, 21, 33, 35, 55\}$.

### 6.2. Variáveis de Resposta

Para quantificar e comparar o desempenho das arquiteturas sob o efeito do ruído quântico real, monitorou-se três variáveis de resposta principais:

- **Profundidade do Circuito (*Circuit Depth*):** Número de fatias temporais sequenciais do circuito. Profundidades maiores estendem o tempo de execução, expondo os qubits por mais tempo à decoerência.
- **Contagem de Portas CNOT:** Quantidade total de operações de dois qubits. Por possuírem taxas de erro ordens de magnitude superiores às de qubit único, as CNOTs atuam como o principal gargalo de fidelidade.
- **Fidelidade de Bhattacharyya e Taxa de Sucesso:** Para capturar a preservação do sinal quântico independentemente do erro de pós-processamento clássico, utilizou-se a *Fidelidade de Bhattacharyya* $F(P_{\text{ruidoso}}, P_{\text{ideal}}) = \left(\sum_i \sqrt{P_{\text{ruidoso}}(i) \cdot P_{\text{ideal}}(i)}\right)^2$, complementada pela proporção de acertos na recuperação do período através do algoritmo clássico de frações contínuas.

### 6.3. Ambiente de Controle e Execução

As execuções em hardware quântico real foram submetidas ao processador `ibm_fez`, um chip baseado na arquitetura de última geração **IBM Heron**. A modelagem dos circuitos e as diretivas de compilação foram gerenciadas via *framework* Qiskit, aplicando o nível máximo de otimização do compilador (`optimization_level=3`) para mitigar a inserção de portas espúrias durante o roteamento topológico.

Como grupo de controle ideal, adotou-se o simulador de estado completo PennyLane. Para assegurar a confiabilidade estatística, contemplar a flutuação temporal inerente ao hardware e minimizar erros de amostragem, todas as execuções físicas foram compiladas e executadas em três repetições independentes ($n = 3$ *jobs*), configuradas rigidamente com 1.024 medições (*shots*) por execução. Por fim, as distribuições e os estados resultantes foram processados para extração das métricas de fidelidade e validação da fatoração.

### 6.4. Resultados e Discussão

A avaliação dos resultados foi estruturada para evidenciar a barreira tecnológica imposta pelo *hardware* NISQ perante o algoritmo de Shor. Esta primeira etapa foca exclusivamente na arquitetura de alta resolução (padrão da literatura, com registo de precisão $m = 2L$), estabelecendo o cenário base (*baseline*) de complexidade e mapeando a degradação do sinal quântico à medida que a instância $N$ aumenta.

#### 6.4.1. Crescimento da Complexidade Quântica e Explosão de Recursos

O principal obstáculo para a viabilidade do algoritmo de Shor em *hardware* real é o valor massivo de operações necessárias para a exponenciação modular. A Figura 3 ilustra o crescimento severo da profundidade do circuito e da contagem de portas CNOT após o processo de transpilação para o processador `ibm_fez`.

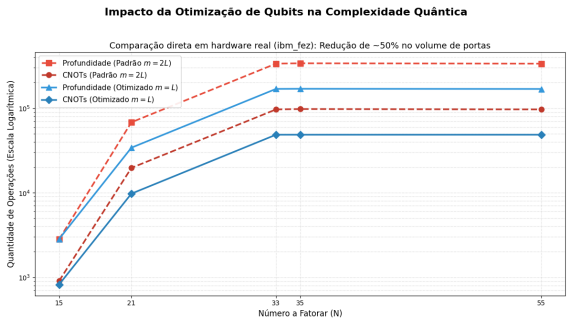


**Figura 3. Crescimento da complexidade quântica: Evolução da profundidade do circuito e da contagem de portas CNOT em função de $N$ (Escala Logarítmica).**

A análise revela que, para a menor instância do problema ($N = 15$), o roteamento lógico-físico gerou un circuito com profundidade de 2.762 fatias temporais e um total de 935 portas CNOT. Embora estes números já sejam elevados para um computador da era NISQ, o limiar de fidelidade das portas do processador Heron permitiu que a assinatura quântica fosse extraída com clareza. No entanto, o escalonamento para instâncias superiores demonstra a intratabilidade do modelo de precisão total em sistemas ruidosos.

No limite do experimento ($N = 55$), a profundidade do circuito atinge a marca de aproximadamente 336.247 operações e o número de portas CNOT ultrapassa as 96,667. Este crescimento é crítico porque as portas CNOT são a principal fonte de ruído nos processadores atuais. Ao atingir este volume de operações, o tempo total de execução do algoritmo supera drasticamente os tempos de coerência ($T_1$ e $T_2$) dos qubits do `ibm_fez`. Como consequência, o estado quântico sofre um colapso antes mesmo de a computação terminar, o que explica a queda acentuada na taxa de sucesso que será discutida na subsecção seguinte.

### 6.4.2. Evolução da Fidelidade e o Muro da Decoerência

Para avaliar o impacto prático da complexidade do circuito na arquitetura padrão ($m = 2L$), o algoritmo foi executado no processador `ibm_fez`. Visando capturar o *drift* de fidelidade inerente aos qubits supercondutores, realizaram-se três repetições independentes ($n = 3$ *jobs*) de $1.024$ *shots* em janelas de calibração distintas. Além disso, aplicou-se a mitigação de erros de leitura TREX (`resilience_level=1` via `SamplerV2`) para isolar a degradação gerada pela profundidade do circuito.

Os dados consolidados da média de três execuções (ilustrados na Figura 10) demonstram o comportamento não-monotônico e a forte degradação imposta pelo "muro da decoerência". Para a instância $N = 15$, o hardware real reteve uma fidelidade média de $27.17\% \pm 5.68\%$.O pico de fidelidade do conjunto foi observado em $N = 21$, atingindo $53.96\% \pm 1.08\%$, o que reflete a retenção parcial da interferência construtiva da QFT em circuitos de complexidade intermediária antes da despolarização total.

No entanto, à medida que a instância do problema avança para $N = 33$, $35$ e $55$, a contagem massiva de portas CNOT e a alta profundidade transpilada elevam a exposição dos qubits à decoerência. Como resultado, a fidelidade de Bhattacharyya despenca para

valores restritos de $8.26\% \pm 0.44\%$ em $N = 33$, $17.19\% \pm 1.19\%$ em $N = 35$, e $14.20\% \pm 0.21\%$ em $N = 55$.

Conforme corroborado pelas distribuições individuais e taxas de sucesso exibidas na Figura 9, a transição para instâncias compostas maiores acentua o impacto do ruído. Enquanto a menor instância ($N = 15$) atinge uma taxa de sucesso prático de $50,7\%$ no pós-processamento clássico, o aumento na complexidade de portas faz com que a taxa de acerto caia de forma abrupta para patamares críticos nas demais instâncias ($7,2\%$ em $N = 21$, $9,7\%$ em $N = 33$, $6,6\%$ em $N = 35$ e $5,7\%$ em $N = 55$).

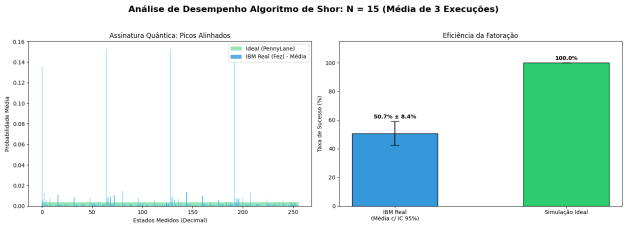


**Figura 4.** $N = 15$ **(50,7%)**

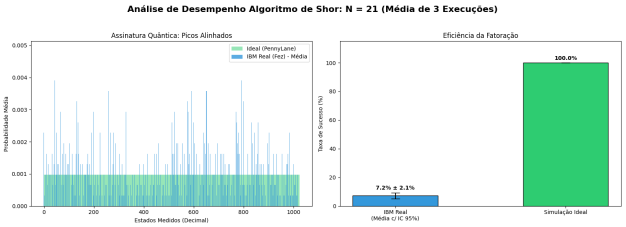


**Figura 5.** $N = 21$ **(7,2%)**

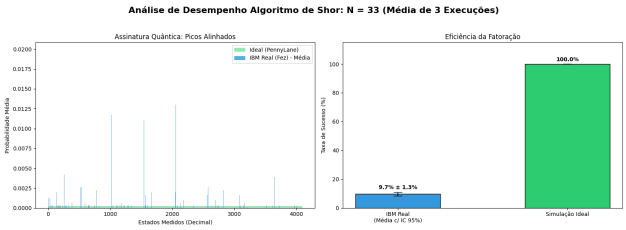


**Figura 6.** $N = 33$ **(9.7%)**

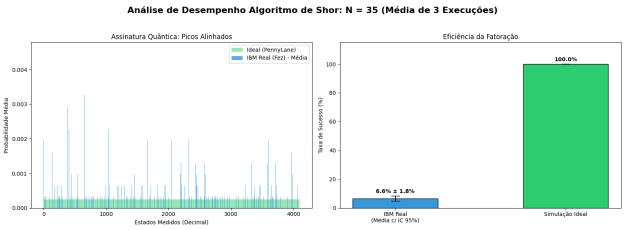


**Figura 7.** $N = 35$ **(6,6%)**

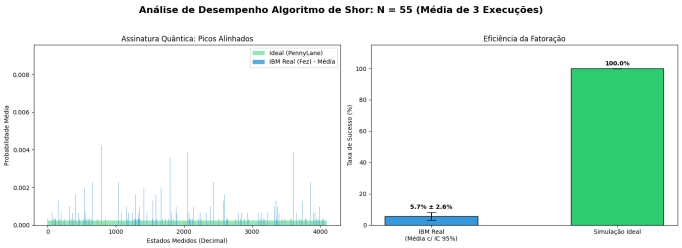


**Figura 8.** $N = 55$ **(5,7%)**

**Figura 9. Desempenho detalhado por instância na arquitetura padrão ($m = 2L$), contrastando a assinatura quântica e a eficiência da fatoração nas execuções físicas.**

Em síntese, os resultados empíricos revelam um claro *trade-off* na execução do algoritmo em hardwares da era NISQ. Embora a alocação de $m = 2L$ qubits garanta o rigor matemático necessário para mitigar o vazamento espectral na Estimativa de Fase Quântica (QPE), o aumento substancial na profundidade do circuito compromete sua viabilidade prática. O acúmulo de falhas nas operações CNOT, aliado à inevitável perda de coerência ditada pelos tempos de relaxamento ($T_1$) e desfasamento ($T_2$) do processador `ibm_fez`, degrada o estado quântico antes que a computação seja concluída. Portanto, a exatidão teórica do modelo padrão acaba severamente limitada pelas restrições físicas do dispositivo, justificando a necessidade de abordagens otimizadas que reduzam o custo do circuito em ambientes ruidosos.

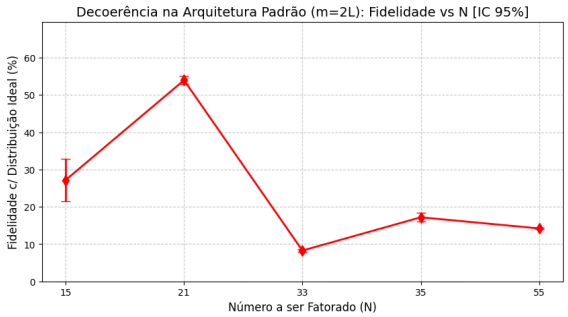


**Figura 10. Preservação do Sinal Quântico na Arquitetura Padrão ($m = 2L$): Fidelidade de Bhattacharyya média em função de $N$ com Intervalo de Confiança de 95%.**

### 6.4.3. Otimização de Recursos: O Compromisso da Arquitetura Reduzida ($m = L$)

Para contornar a rápida degradação do estado quântico observada no modelo de alta resolução, a segunda etapa do experimento avaliou a arquitetura otimizada, reduzindo o registrador de fase para $m = L$ qubits. Esta abordagem diminui drasticamente a profundidade do circuito e a contagem de portas CNOT, mitigando a exposição da informação ao ruído de decoerência e aos erros operacionais do processador `ibm_fez`. O custo intrínseco dessa otimização espacial é a introdução do chamado vazamento espectral (*spectral leakage*), que fragmenta a probabilidade de leitura caso o período $r$ não seja uma potência exata de base 2.

Para quantificar esse novo *trade-off* na prática, as instâncias foram submetidas ao mesmo regime de três repetições independentes com $1.024$ *shots*. A Figura 19 contrasta os resultados da preservação do sinal quântico (Fidelidade) e a eficiência prática da fatoração (Taxa de Sucesso).

Os dados empíricos consolidados confirmam que a redução estrutural do circuito proporcionou um salto expressivo na retenção da integridade quântica. A fidelidade do sinal alcançou $61,1\%$ em $N = 15$, atingindo um pico notável de $97,8\%$ para a instância $N = 21$. Mesmo nas instâncias de maior complexidade algébrica, a sobrevivência do estado quântico manteve-se superior ao cenário padrão, registrando $71,8\%$ em $N = 33$, $46,3\%$ em $N = 35$ e retendo consideráveis $30,5\%$ em $N = 55$.

Apesar do notório ganho de proteção contra a decoerência, a análise das taxas de sucesso prático, detalhadas na Figura 16, revela a pesada limitação imposta pelo truncamento de fase. Para $N = 15$, o sucesso de fatoração atingiu $61,2\% \pm 2,0\%$, refletindo um alinhamento harmônico parcial com o registrador reduzido[cite: 3]. Em contrapartida, as demais instâncias ilustram o impacto severo do vazamento espectral no pós-processamento clássico. O caso de $N = 21$ é emblemático: embora a fidelidade física tenha beirado a perfeição ($97,8\%$), a taxa de sucesso desabou para apenas $2,8\% \pm 0,9\%$. O mesmo comportamento limitante foi aferido em $N = 33$ ($6,8\% \pm 2,3\%$) e $N = 35$ ($1,2\% \pm 0,5\%$), com uma ligeira elevação não linear em $N = 55$, que registrou sucesso de $13,0\% \pm 2,4\%$.

Um aspecto contra-intuitivo que emerge da análise é o desempenho da simulação ideal, que chega a ser matematicamente superado pelas execuções no hardware físico rui-

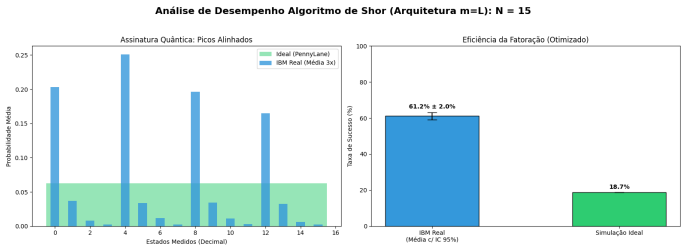


**Figura 11.** $N = 15$ **(Fidelidade: 61,1% — Sucesso: 61,2%)**

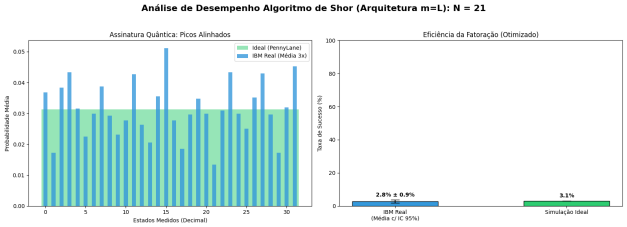


**Figura 12.** $N = 21$ **(Fidelidade: 97,8% — Sucesso: 2,8%)**

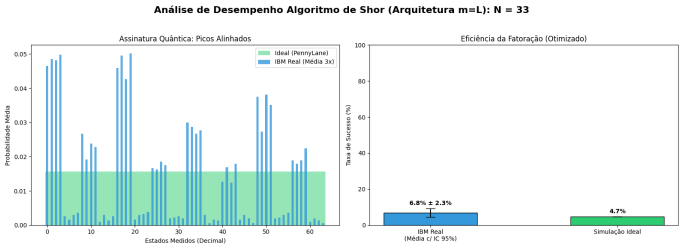


**Figura 13.** $N = 33$ **(Fidelidade: 71,8% — Sucesso: 6,8%)**

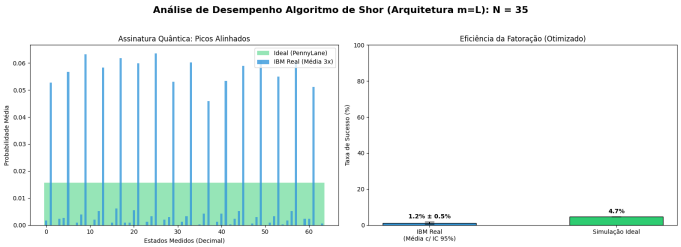


**Figura 14.** $N = 35$ **(Fidelidade: 46,3% — Sucesso: 1,2%)**

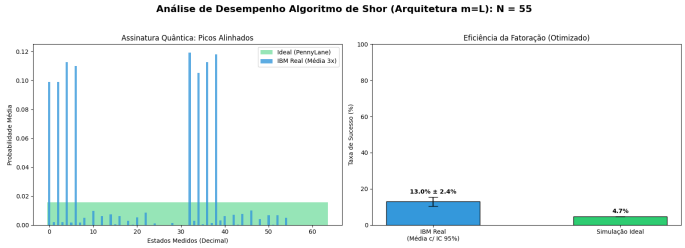


**Figura 15.** $N = 55$ **(Fidelidade: 30,5% — Sucesso: 13,0%)**

**Figura 16. Desempenho detalhado por instância na arquitetura otimizada ($m = L$), contrastando a integridade quântica (picos alinhados) versus a eficiência prática de fatoração.**

doso em instâncias como $N = 15$ e $N = 55$. Devido ao tamanho restrito da amostra ($n = 3$ execuções físicas por instância), a robustez estatística dessa variação exige cautela interpretativa, não devendo ser cravada como uma regra absoluta de escalonamento. Contudo, este comportamento pontual não reflete uma anomalia do simulador, mas evidencia um efeito gerado pela interação tangível entre a despolarização física e a limitação algorítmica da arquitetura de resolução reduzida.

Na ausência de ruído cenário verificado ao focar os testes da simulação em modo puramente clássico com *threads* dedicadas, sem emulação quântica o estado exibe perfeição algébrica. Entretanto, ao reduzir o registrador de contagem para $m = L$, o circuito perde a resolução necessária para codificar fases que não sejam frações exatas de potências de base 2. O decorrente vazamento espectral (*spectral leakage*) fragmenta as amplitudes de probabilidade teóricas em picos rígidos e determinísticos que, com enorme frequência, não convergem para o período $r$ correto durante a etapa do algoritmo clássico de frações

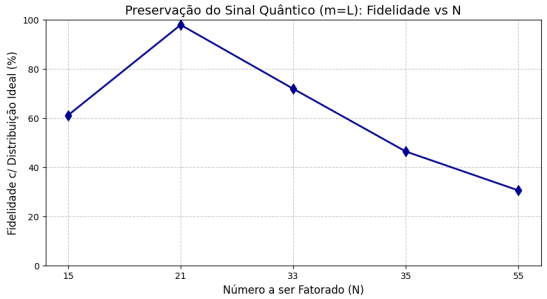


**Figura 17. Preservação do Sinal Quântico na arquitetura otimizada ($m = L$).**

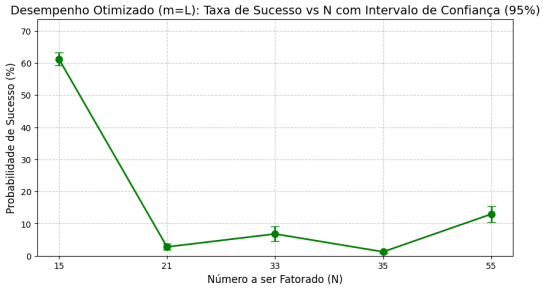


**Figura 18. Taxa de Sucesso vs $N$ na arquitetura otimizada com Intervalo de Confiança (95%).**

**Figura 19. Avaliação global de desempenho (Fidelidade e Sucesso) para a arquitetura otimizada ($m = L$).**

contínuas.

Por outro lado, as execuções físicas no processador `ibm_fez` sofrem intensa influência de instabilidade térmica intrínseca à supercondutividade. De forma paradoxal, esse ruído atua como um canal despolarizador que ”achata”a distribuição. Em vez de uma dispersão espectral perfeitamente localizada, o ruído distribui as probabilidades para estados adjacentes. Devido à natureza sensível da lógica de busca de período na parte clássica do fluxograma, alguns desses estados vizinhos agora favorecidos pelo espalhamento térmico acabam satisfazendo as condições matemáticas de convergência. Trata-se de um fenômeno onde a despolarização do hardware atenua temporariamente a degradação lógica imposta pelo truncamento espectral, elevando artificialmente a taxa de sucesso no pós-processamento.

Em conclusão, a análise revela que a topologia otimizada não soluciona definitivamente a viabilidade do algoritmo de Shor na era NISQ, mas sim atua como um mecanismo de transferência de gargalo. Enquanto o modelo padrão ($m = 2L$) esbarra nas limitações físicas do hardware (decoerência), a arquitetura enxuta transfere o obstáculo para o domínio lógico-algorítmico, onde o espalhamento da fase quântica inviabiliza a resolução clássica eficiente.

## 7. Considerações Finais

Este trabalho preenche uma lacuna prática ao confrontar a ameaça teórica do algoritmo de Shor com as limitações empíricas do processador **IBM Heron** (`ibm_fez`) em instâncias escaladas até $N = 55$. Os resultados quantificaram o impacto severo do ruído na era NISQ e evidenciaram um claro *trade-off* arquitetural: enquanto o modelo padrão ($m = 2L$) esbarra no “muro da decoerência” devido à explosão de portas CNOT, a configuração otimizada de registrador reduzido ($m = L$) eleva expressivamente a integridade física do sinal quântico (alcançando $97,8\%$ de fidelidade em $N = 21$), transferindo contudo o gargalo para o domínio lógico-algorítmico por meio do vazamento espectral no pós-processamento clássico.

Para profissionais de cibersegurança e gestores de infraestrutura, os dados fornecem uma base factual para o planejamento da migração à Criptografia Pós-Quântica

(PQC) livre de alarmismos. Embora o hardware atual esteja longe de ameaçar chaves comerciais, a adoção de estratégias de *crypto-agility* mostra-se imperativa para mitigar o vetor de ataque *Harvest Now, Decrypt Later* (Coletar Agora, Decifrar Depois).

Como desdobramentos e trabalhos futuros, propõe-se: validar o algoritmo de Shor em plataformas de íons aprisionados e átomos neutros, contrastando diferentes tempos de coerência e topologias de conectividade; implementar e testar o algoritmo de Grover em hardware real, avaliando experimentalmente o impacto do ganho quadrático e dos limites de profundidade na quebra de primitivas simétricas como o AES; investigar métodos alternativos de estimação de fase e pós-processamento híbrido (como o algoritmo de Regev) para mitigar o vazamento espectral e reduzir ainda mais a dependência de portas de dois qubits.

Em suma, este estudo corrobora a ideia de que as atuais limitações de hardware NISQ restringem significativamente a execução prática do algoritmo de Shor, oferecendo métricas empíricas que subsidiam o planejamento da migração para criptografia pós-quântica com base em dados concretos.

Como compromisso com a transparência e a reprodutibilidade científica, todo o conjunto de scripts de transpilação desenvolvidos para este trabalho encontra-se acessível em `https://github.com/lluis50045/Shor-s-Algorithm-Implementation-via-Qiskit`.

## Agradecimentos

Os autores integram o subgrupo de Computação Quântica do grupo de pesquisa em ”Algoritmos, Otimização, Inteligência e Complexidade Computacional”(ALGOX) do Programa de Pós-Graduação em Informática da UFAM e do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) e também integram a Rede IATQ (Projeto Pró-Defesa V em Inteligência Artificial e Tecnologias Quânticas). A pesquisa foi realizada com o apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES-PROEX) – Código de Financiamento 001, bem como financiada parcialmente pela Fundação de Amparo à Pesquisa do Estado do Amazonas (FAPEAM), por meio dos projetos DPG-CAPES, POSGRAD 2025-2026 e POSGRAD 2026-2027.

## Referências

Abdel-Rehim, W. M. F. (2025). The impact of quantum noise on Shor's algorithm and its cryptographic applications. In *2025 15th International Conference on Electrical Engineering (ICEENG)*, pages 1–6. IEEE.

Amico, M. (2026). Exponentially cheaper coherent phase estimation via uncontrolled unitaries. *arXiv preprint arXiv:2603.27858v2*.

Amico, M., Saleem, Z. H., and Kumph, M. (2019). An experimental study of shor's factoring algorithm on ibm q. *Physical Review A*, 100(1):012305.

Bagourd, P. et al. (2026). Practical challenges in executing shor's algorithm on existing quantum platforms. *arXiv preprint arXiv:2512.15330v3*.

Dubey, V. M. and Varshney, G. (2026). Measurement study of post-quantum readiness of internet: 2026.

Dutkiewicz, A. et al. (2025). Error mitigation and circuit division for early fault-tolerant quantum phase estimation. *arXiv preprint arXiv:2410.05369v2*.

Gidney, C. (2025). How to factor 2048 bit rsa integers with less than a million noisy qubits.

Gidney, C. and Ekerå, M. (2021). How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum*, 5:433.

Kahanamoku-Meyer, G. D. et al. (2025). A log-depth in-place quantum fourier transform that rarely needs ancillas. *arXiv preprint arXiv:2505.00701*.

Kavitha, S. S. et al. (2025). Quantum shor's algorithm vs. classical general number field sieve (gnfs) approach for large integer factorization. In *2025 International Conference on Next Generation Communication & Information Processing (INCIP)*, pages 1–6. IEEE.

Lee, Y., Choi, M., Min, Y., Bae, E., and Bae, S. (2025). Two variations of quantum phase estimation for reducing circuit error rates: Application to the harrow-hassidim-lloyd algorithm. *arXiv preprint arXiv:2507.06711*.

Lenstra, A. K. and Lenstra, H. W. (1993). *The development of the number field sieve*. Springer-Verlag, Berlin.

Mallick, T., Zeldin, M., Cenk, M., and Nita-Rotaru, C. (2025). Quantum disruption: An sok of how post-quantum attackers reshape blockchain security and performance.

National Institute of Standards and Technology (2024). Post-quantum cryptography standardization. NIST Computer Security Resource Center.

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

Rassekhnia, J. (2026). Quantum encryption resilience score (qers) for computer system processes, iot, and iiot devices across mqtt, http, and https.

Robertson, R. and Ventura, D. (2024). Introducing unique: The unconventional noiseless intermediate quantum emulator. *arXiv preprint arXiv:2409.07000*.

Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134. IEEE.

Skosana, U. and Tame, M. (2022). Demonstration of shor's factoring algorithm for $n = 21$ on ibm quantum processors. *arXiv preprint arXiv:2103.13855*.

Su, T. H. et al. (2026). Scalable quantum reinforcement learning on nisq devices with dynamic-circuit qubit reuse. *arXiv preprint arXiv:2509.16002v2*.

Zelenovic, J., Taghizadeh, L., Pena-Gonzalez, E., García, J. G., and Preneel, B. (2026). Post-quantum discovery as a governance capability: Evidence-based cryptographic visibility and exposure prioritisation in a critical service provider.