Table of Contents

A GEOMETRIA OCULTA DO TEMPO COMPUTACIONAL

Da barreira subexponencial da fatoração de inteiros à soberania pós-quântica — e o caso das funções mock theta como primitiva criptográfica

Marcos Eduardo Elias

Holosystems Quantum Computing · Post Quantum Sistemas Criptográficos Avançados · Θ-Crypt Brasil

São Paulo, junho de 2026

Resumo

A segurança da criptografia de chave pública contemporânea repousa sobre uma assimetria computacional precisa: multiplicar dois primos é trivial; recuperá-los a partir do produto é, até onde se sabe classicamente, intratável em escala. Este artigo reconstrói, com profundidade histórica e rigor analítico, a anatomia dessa intratabilidade — não como um fato bruto, mas como uma *geometria*. Mostramos que o custo de fatorar não se distribui em duas categorias ingênuas ("fácil" e "difícil"), mas em quatro regimes de complexidade, cada um com uma curva de custo de forma distinta: a parede exponencial de Pollard, o arco subexponencial de Lenstra e do crivo, e o piso polinomial de Shor. A tese central, que organiza todo o texto, é que *aceleradores físicos — silício dedicado, energia, paralelismo — deslocam a curva de custo por um fator constante, mas jamais alteram sua inclinação; e a inclinação é a*

classe de complexidade. Daí decorre que nenhuma engenharia clássica transpõe a barreira do expoente $\alpha = 1/3$ do crivo de corpos numéricos, intransposta há mais de três décadas; apenas a ruptura quântica o faz, rebaixando a inclinação ao chão polinomial. Calibramos os quatro regimes numa base consistente e os destilamos num diagnóstico operacional (Figura 1). Estabelecida a paisagem, voltamo-nos para a fronteira viva — a transição pós-quântica e o imperativo de soberania criptográfica — e culminamos na única seção que reivindica originalidade matemática genuína: a proposta de empregar as *funções mock theta* de Ramanujan, compreendidas, após Zwegers (2002), como as partes holomorfas de formas de Maass harmônicas de peso 1/2, como primitiva criptográfica estruturalmente distinta, ancorada no princípio de *não-identificabilidade* em vez da dureza computacional convencional. Apresentamos o arcabouço com entusiasmo e, sobretudo, com a honestidade que o assunto exige: suas reduções de segurança permanecem em aberto, e seu uso responsável é estritamente híbrido.

I. Introdução: o pilar que é também a ameaça

Toda a confiança depositada diariamente em trilhões de transações cifradas assenta sobre uma frase de Gauss, nas *Disquisitiones Arithmeticae* de 1801, que ele tratava como um problema de dignidade quase estética: *distinguir números primos de compostos, e resolver estes últimos em seus fatores primos, é reconhecido como um dos mais importantes e úteis da aritmética*. Gauss não podia prever que duzentos anos depois essa "dignidade" se converteria em infraestrutura — que o sistema RSA de Rivest, Shamir e Adleman (1977) faria da dificuldade de fatorar a fechadura da economia digital. Mas a intuição estava correta: a fatoração é simultaneamente um dos problemas mais antigos e mais consequentes da matemática.

O que torna o problema tão fértil é uma assimetria. A multiplicação é uma operação de tempo quase linear; a fatoração, no estado da arte clássico, é subexponencial. RSA é a monetização dessa fenda. E é precisamente por isso que entender *a forma exata* da dificuldade — não apenas que ela existe, mas como ela escala, onde estão suas paredes e suas frestas — é uma questão de soberania, não de curiosidade.

Este artigo persegue essa forma. A Parte clássica (Seções II–VIII) é um levantamento — denso, mas levantamento — do que a humanidade sabe sobre fatorar, organizado pela ideia de que cada método *é* uma geometria de custo. A Parte de fronteira (Seção IX) situa o leitor no momento presente: a padronização pós-quântica e o imperativo de diversificação. E a Parte original (Seção X) apresenta a aposta de invenção genuína — as funções mock theta como primitiva —, claramente demarcada de tudo o que a precede, porque a integridade intelectual exige distinguir o que se domina do que se descobre.

II. A anatomia da dificuldade: a notação L e a lei de Dickman

O primeiro erro a desfazer é a palavra "exponencial". O crivo de corpos numéricos, o melhor algoritmo clássico conhecido, **não** é exponencial. Ele é *subexponencial*, e a

distinção é toda a história. A linguagem para expressá-la é a notação L de Carl Pomerance:

$$L_N[\alpha, c] = \exp\Big(\big(c + o(1)\big)\,(\ln N)^{\alpha}\,(\ln\ln N)^{1-\alpha}\Big).$$

O parâmetro $\alpha \in [0,1]$ interpola entre dois mundos. Em $\alpha = 1$, $L_N[1, c] = N^c$ a menos de fatores — crescimento *exponencial* no tamanho de N. Em $\alpha = 0$, $L_N[0, c] = (\ln N)^c$ — crescimento *polinomial*. Todo o drama da fatoração clássica vive no interior aberto do intervalo, e o número que importa não é a constante c, mas o expoente α: é ele que define a *classe* da curva.

A maquinaria analítica que governa esses expoentes é a teoria dos números *smooth* (lisos), e seu objeto central é a função ρ de Dickman–de Bruijn. Um inteiro é B-smooth se todos os seus fatores primos são $\leq B$. Karl Dickman, num artigo de 1930 hoje célebre, mostrou que a probabilidade de um inteiro $\leq x$ ser y-smooth tende a $\rho(u)$, onde $u = \ln x/\ln y$ e ρ satisfaz a equação diferencial-de-retardo

$$u\,\rho'(u) = -\,\rho(u-1), \qquad \rho|_{[0,1]} \equiv 1,$$

com a assintótica $\rho(u) = u^{-u(1+o(1))}$. O teorema de Canfield–Erdős–Pomerance (1983) converteu essa lei probabilística no princípio de projeto de todo método subexponencial: existe um tamanho de base de fatores que equilibra o custo de procurar relações *smooth* contra o custo de processá-las, e otimizar contra ρ *é* otimizar o algoritmo. Dominar a função de Dickman é dominar o coração heurístico do campo — e é o estrato analítico que quase nenhum praticante de criptografia domina de fato.

III. O primeiro paradigma: métodos de ordem fixa e a parede $\sqrt{p}$

Os métodos da primeira geração compartilham uma assinatura estrutural: seu custo é governado por um grupo de *ordem fixa*. Pierre de Fermat, no século XVII, observou que todo composto ímpar $N = ab$ se escreve como diferença de quadrados $N = s^2 - t^2 = (s-t)(s+t)$, reduzindo a fatoração à busca de um quadrado perfeito na sequência $s^2 - N$. Legendre e Gauss refinaram a ideia em direção às formas quadráticas e às congruências de quadrados — o germe distante do crivo.

A virada algorítmica moderna veio com John Pollard. Seu método $p-1$ (1974) explora o pequeno teorema de Fermat: se todo fator primo de $p-1$ é $\leq B$, então $a^M \equiv 1\ (mod\ p)$ para $M = lcm(1, \dots, B)$, e $\gcd(a^M - 1, N)$ revela p. O método rho (1975) — batizado pela forma da letra grega que o ciclo de colisões desenha — usa o paradoxo do aniversário sobre a iteração $x \mapsto x^2 + c\ mod\ N$ para encontrar um fator p em $O\big(\sqrt{p}\big)$ passos. Hugh Williams (1982) acrescentou o método $p+1$, trabalhando na ordem $p+1$ via sequências de Lucas.

O defeito é comum e fatal. Cada método está preso a *um único grupo* de *ordem aritmeticamente fixa* — $p-1$, ou $p+1$, ou a ordem do ciclo rho. Se esse número específico não for *smooth*, não há recurso: trocar a base não muda a ordem. É um

sorteio com um único bilhete. E o custo $\sqrt{p}$ do rho, embora pareça modesto, é **exponencial no número de bits do fator**: $\sqrt{p} = \exp\left(\frac{1}{2}\ln p\right) = \exp\left(\frac{1}{2}(\ln 2)\,\beta\right)$ para $\beta = \log_2 p$ bits. Numa escala logarítmica de tempo, isto é uma reta de inclinação máxima — a *parede* que, no diagnóstico final, cruza a idade do universo antes mesmo de o fator atingir sessenta dígitos. O método "simples" morre cedo, e morre pela geometria.

IV. O grande salto: $\alpha = 1/2 \to \alpha = 1/3$ e a barreira intransposta

A revolução do campo — a única mudança de *classe* na história clássica da fatoração — foi a passagem de $\alpha = 1/2$ para $\alpha = 1/3$. A família de $\alpha = 1/2$ nasceu do crivo quadrático de Pomerance (1981), que sistematizou a busca de congruências de quadrados $x^2 \equiv y^2 \ (mod\ N)$ peneirando valores de um polinômio quadrático por *smoothness* e combinando-os por álgebra linear sobre $GF(2)$. O crivo quadrático fatorou os números mais difíceis de sua época e roda em $L_N[1/2,1]$.

O salto para $\alpha = 1/3$ veio do crivo de corpos numéricos (NFS). A semente é de Pollard (1988), numa carta manuscrita circulada entre especialistas; a teoria foi desenvolvida por A. K. Lenstra, H. W. Lenstra Jr., Mark Manasse e John Pomerance, e a análise de complexidade por Joe Buhler, H. W. Lenstra e Pomerance. A ideia é profunda: em vez de peneirar inteiros, peneira-se sobre o *anel de inteiros de um corpo de números* $\mathbb{Q}(\theta)$, onde as "normas" dos elementos são valores de um polinômio cuidadosamente escolhido, e a *smoothness* dessas normas é muito mais provável do que a de inteiros do tamanho de N. O resultado é a complexidade

$$L_N\left[\frac{1}{3},\ (64/9)^{1/3}\right], \qquad (64/9)^{1/3} \approx 1{,}923,$$

para o NFS geral (GNFS), e $(32/9)^{1/3} \approx 1{,}526$ para o crivo especial (SNFS), aplicável a números de forma algébrica privilegiada como os de Cunningham.

Aqui está o fato que define a fronteira clássica inteira: **o expoente $\alpha = 1/3$ jamais foi reduzido.** Don Coppersmith mostrou em 1993 que, com múltiplos corpos numéricos e pré-computação, a *constante* cai para $\approx 1{,}902$ — mas α não se moveu. Em mais de trinta anos, ninguém exibiu um algoritmo clássico $L_N[1/4, \cdot\,]$, e a suspeita predominante entre os teóricos é que fazê-lo exigiria uma ideia tão profunda quanto o próprio crivo. Esta é a *barreira subexponencial*: a parede contra a qual toda engenhosidade individual eventualmente se choca.

O que *resta* mover, e onde a arte real do NFS vive, é a constante e o termo $o(1)$ — e a alavanca de maior retorno é a **seleção de polinômio**. A tese de Brian Murphy (Australian National University, 1999) formalizou a função de aptidão hoje canônica, o *Murphy-E score*, que estima o rendimento de relações de um par de polinômios como uma quadratura do integral de *smoothness* governado por ρ, corrigido por dois fatores: a *skewness* (a geometria anisotrópica ótima da região de crivo) e o $\alpha(f)$ de correção de raízes (que mede quão mais divisíveis por primos pequenos os valores do polinômio são, em comparação com inteiros aleatórios). Thorsten Kleinjung

transformou a busca por bons polinômios numa indústria, e é graças a ela que recordes como o RSA-250 (250 dígitos, ≈ 2,700 core-anos de CPU, 2020) foram atingidos. Mas note: tudo isso comprime c e $o(1)$. O 1/3 permanece soberano.

V. ECM: a fatoração governada pelo fator

Em 1985, Hendrik Lenstra introduziu o método das curvas elípticas (ECM) com uma ideia de limpeza ímpar: *substituir um grupo de ordem fixa por uma família de grupos cuja ordem se pode re-sortear*. Onde Pollard estava preso à ordem fixa $p-1$, Lenstra trabalha no grupo de pontos $E(\mathbb{F}_p)$ de uma curva elíptica, cuja ordem, pelo teorema de Hasse,

$$\#E(\mathbb{F}_p) = p + 1 - a_p, \qquad |a_p| \le 2\sqrt{p},$$

varia no *intervalo de Hasse* à medida que se troca de curva. Cada nova curva é um novo bilhete de loteria: persiste-se trocando E até cair numa cuja ordem seja *smooth*. A degenerescência do bilhete único desaparece.

O mecanismo de extração é de uma beleza algébrica particular. Executa-se a aritmética sobre $\mathbb{Z}/N\mathbb{Z}$ — que não é corpo — sem conhecer p; quando a ordem reduzida módulo p divide o escalar, o ponto reduzido atinge o infinito, a inversão da lei de grupo *falha*, e o denominador que não se pode inverter revela $\gcd(\cdot, N) = p$. A falha de inversão não é um acidente a contornar: é o próprio instrumento. Uma derivação direta, equilibrando o custo por curva ($\sim B_1$ operações de grupo) contra o número esperado de curvas ($\sim 1/\rho(u)$), entrega a complexidade

$$C_{\text{ECM}} = L_p\left[\frac{1}{2}, \sqrt{2}\right] \cdot poly(\log N).$$

A leitura estrutural é tudo: o termo subexponencial depende de p, o *fator procurado*, e não de N. Nenhum outro método de propósito geral tem essa propriedade. Daí as duas vocações do ECM — campeão para fatores de tamanho médio (o recorde público é de 83 dígitos, R. Propper, 2013, ainda imbatido) e sub-rotina ideal de *cofatoração* dentro do próprio NFS, onde os fatores buscados são pequenos por construção.

A engenharia que tornou o ECM um cavalo de batalha é uma genealogia em si. Peter Montgomery (1987) introduziu a forma de curva e a "escada" que executa multiplicação escalar usando apenas a coordenada x, sem inversões no caminho. A parametrização de Suyama força fatores pequenos conhecidos na ordem do grupo, melhorando a probabilidade de *smoothness*. E Bernstein, Birkner, Lange e Peters (2008) migraram para as curvas de Edwards torcidas com $a = -1$, cuja lei de adição é *completa* — sem casos excepcionais, sem ramificação dependente de dados —, o que as torna o objeto ideal para paralelização massiva em GPU, FPGA e ASIC. É exatamente nesse ponto que a matemática encontra o silício: um acelerador de cofatoração ECM, com aritmética modular em representação de resíduos (datapath Cox–Rower de Kawamura–Nozaki, 2000), foi o precedente real das máquinas COPACOBANA/RIVYERA de Bochum. E aqui registra-se a honestidade desconfortável que a literatura impõe (de Meulenaer e colegas): tais aceleradores *mal* superam

software bem-afinado em GPU numa base normalizada por custo; sua vantagem real é energética — modmul por Watt —, não bruta. O hardware dedicado desloca a curva para baixo por um fator constante. Não muda sua inclinação.

VI. Quando a estrutura vaza: Coppersmith, reticulados e canais laterais

Há uma terceira via, ortogonal às duas anteriores, e ela muda a natureza do jogo. Os métodos do crivo e do ECM atacam N de frente, ignorando qualquer estrutura particular de p. O método de Don Coppersmith (1996) faz o oposto: *assume que se conhece parte da informação sobre* p — bits altos, bits baixos, um fator comum — e converte esse conhecimento parcial em fatoração completa em tempo **polinomial**.

A ferramenta é a redução de reticulado, e seu fundamento é o algoritmo LLL de Arjen Lenstra, Hendrik Lenstra e László Lovász (1982) — um dos algoritmos mais consequentes do século XX, que encontra vetores curtos numa base de reticulado em tempo polinomial. A reformulação de Nick Howgrave-Graham (1997) tornou a ideia transparente: para recuperar uma raiz pequena x_0 de um polinômio módulo um divisor desconhecido $b \mid N$, fabrica-se uma combinação de polinômios que se anulam módulo uma potência alta b^m e cujos coeficientes são tão pequenos que o valor, calculado sobre os inteiros, é menor que b^m — forçando-o a ser *zero sobre* $\mathbb{Z}$. A congruência módulo o divisor invisível vira uma equação inteira visível. A otimização entrega o limiar célebre: para RSA balanceado, conhecer **metade dos bits mais altos de** p ($N^{1/4}$ de incerteza residual) basta para fatorar em tempo polinomial. Para RSA-1024, são 256 bits.

Coppersmith é a base de uma família de ataques que exploram informação parcial: a recuperação de expoente privado pequeno de Boneh–Durfee (1999, $d < N^{0{,}292}$), a fatoração implícita de May–Ritzenhofen, e — crucialmente para a engenharia de canal lateral — a reconstrução de chave de Nadia Heninger e Hovav Shacham (2009). Onde Coppersmith devora bits *contíguos*, Heninger–Shacham devora bits *esparsos*: dado conhecimento de posições aleatórias de cerca de 27% dos bits das cinco quantidades de uma chave RSA-CRT, um algoritmo de ramificação-e-poda reconstrói a chave inteira em tempo esperado polinomial. O modelo de erro correspondente, de Henecka, May e Meurer (2010), tolera uma taxa de corrupção até o limiar informacional $\varepsilon \leq H^{-1}(1 - 1/m)$ — $\approx 24\%$ para os cinco componentes. E o caso degenerado mais elegante é o ataque de falha única de Boneh, DeMillo e Lipton (o ataque "Bellcore"): induzindo *um* erro durante a recombinação CRT de uma assinatura RSA, a assinatura defeituosa s' satisfaz $\gcd(s - s', N) = p$. Nem reticulado, nem busca — um único gcd. É o análogo físico da inversão que falha no ECM: o hardware não quebra a matemática, ele injeta a inconsistência que faz p cair de graça.

A lição estratégica desta seção é precisa: Coppersmith e seus descendentes não comprimem o expoente nem o transpõem — eles o *dispensam*, ao custo de exigir informação que apenas o acesso físico ou lógico ao alvo fornece. É a via mais barata por ordens de magnitude *quando aplicável*. Mas ela quebra implementações, não o problema da fatoração; um RSA de tempo constante, bem-blindado, e um número *frio* dado isoladamente não oferecem fresta alguma.

VII. A ruptura quântica: o expoente que finalmente cai

Tudo o que precede respeita a barreira do $\alpha = 1/3$. O único lugar onde o expoente de fato cai — onde a *inclinação* da curva muda de classe — é o regime quântico, e essa é a notícia que reorganiza toda a estratégia de longo prazo.

Peter Shor, em 1994, exibiu um algoritmo quântico que fatora em tempo *polinomial* em $\log N$. O coração é a redução da fatoração à determinação da ordem de um elemento módulo N, resolvida pela transformada quântica de Fourier que extrai a periodicidade de uma superposição. Shor reduziu o problema de $\alpha = 1/3$ a $\alpha = 0$ — da parede subexponencial ao chão polinomial. Desde então, a questão nunca foi a complexidade assintótica; foi sempre o *custo de recursos tolerantes a falhas*.

E esse custo colapsou em ciclos. A estimativa de Austin Fowler e colaboradores (2012) requeria cerca de um bilhão de qubits físicos. Craig Gidney e Martin Ekerå (2019) a reduziram a $\approx$ 20 milhões de qubits operando por oito horas, combinando a redução de Ekerå–Håstad (fatoração via um único *short discrete-log*), a aritmética de Gidney–Fowler e o código de superfície. E em maio de 2025, no artigo "How to factor 2048 bit RSA integers with less than a million noisy qubits", Gidney estimou que um inteiro RSA de 2048 bits poderia ser fatorado em menos de uma semana por um computador quântico com menos de um milhão de qubits ruidosos — uma redução de 20× na contagem de qubits frente à sua própria estimativa de 2019. O ganho vem da aritmética de resíduos aproximada de Chevignard–Fouque–Schrottenloher (2024), do armazenamento de qubits ociosos com yoked surface codes, e da redução de mais de 100× na contagem de portas Toffoli — engenharia aritmética esperta, não força bruta de hardware.

Mas o desenvolvimento que merece atenção teórica máxima é a **linha de Oded Regev**. Em 2023, Regev reformulou Shor como uma variante de dimensão d: elevando os quadrados dos primeiros $d \approx \sqrt{n}$ primos a expoentes curtos, obtém uma redução do *tamanho do circuito* por um fator $\Theta(\sqrt{n})$ frente às variantes de Shor — um circuito de $\tilde{O}(n^{3/2})$ portas, executado $\sqrt{n} + 4$ vezes, com pós-processamento clássico por redução de reticulado (LLL/BKZ). É um algoritmo *híbrido* em sentido próprio: amostragem quântica seguida de geometria de reticulado clássica. A cadeia de refinamentos é instrutiva: Ragavan e Vaikuntanathan reduziram o espaço a $\tilde{O}(n)$ qubits via exponenciação à la Fibonacci; Pilatte (2024) *provou*, com teoria analítica dos números, a hipótese de que o algoritmo de Regev dependia, tornando-o incondicionalmente correto; e Ekerå–Gärtner estenderam o esquema ao logaritmo discreto. O expoente *de portas*, não apenas o de tempo, está em queda — e está em queda por matemática, não por silício.

VIII. Síntese: o mapa de quatro regimes e a tese da geometria

Reunindo os quatro paradigmas numa base de custo consistente — todos medidos em segundos de parede, os três clássicos sobre uma mesma máquina von Neumann de referência ($W = 10^{15}$ operações de palavra por segundo, da ordem de 10^5 núcleos), e

o quântico sobre um computador tolerante a falhas hipotético sob as hipóteses de Gidney-2025 — obtém-se o diagnóstico da Figura 1.

Figura 1. Custo de fatorar N=p_1p_2p_3 (três primos iguais de D dígitos), nas quatro abordagens, na mesma máquina. Eixo vertical em escala logarítmica. As três curvas clássicas estão sobre uma máquina von Neumann de W=10^{15} word-ops/s; a curva quântica (tracejada) sobre um computador tolerante a falhas hipotético. A faixa colorida inferior indica o método mais rápido em cada tamanho. O ponto branco marca o cruzamento em que o quântico ultrapassa todo o clássico.

Figura 1. Custo de fatorar $N = p_1 p_2 p_3$ (três primos iguais de D dígitos), nas quatro abordagens, na mesma máquina. Eixo vertical em escala logarítmica. As três curvas clássicas estão sobre uma máquina von Neumann de $W = 10^{15}$ word-ops/s; a curva quântica (tracejada) sobre um computador tolerante a falhas hipotético. A faixa colorida inferior indica o método mais rápido em cada tamanho. O ponto branco marca o cruzamento em que o quântico ultrapassa todo o clássico.

A figura é a teoria da complexidade tornada geometria, e cada curva *é* a sua classe. O **Pollard rho** (vermelho) é uma parede quase vertical: exponencial nos bits do fator. O **ECM** (verde) e o **GNFS** (amarelo) são arcos suaves, subexponenciais, quase coincidentes. E o **quântico** (azul tracejado) é quase horizontal: polinomial, um piso. Três formatos, três classes — a parede, o arco, o chão.

Uma nuance que a figura revela e que corrige uma intuição comum: para N produto de três primos *iguais*, o fator é sempre $N^{1/3}$, uma razão fixa, e nesse regime ECM e GNFS correm emparelhados (verde ≈ amarelo), com o GNFS marginalmente à frente para N grande — a vantagem célebre do ECM, "explorar fatores pequenos", só se manifesta

quando o fator é muito menor que $N^{1/3}$ em termos absolutos. No alvo concreto de três primos de cem dígitos ($N \approx 300$ dígitos, ~ 996 bits), leem-se as quatro alturas: rho em $\sim 10^{30}$ anos, ECM em ~ 80 anos, GNFS em $\sim 2{,}6$ anos, quântico em ~ 19 horas. O número está firmemente na zona onde só o chão azul vence — e o chão azul exige hardware tolerante a falhas que ainda não existe. O cruzamento em que o quântico ultrapassa o clássico ocorre por volta de ~ 714 bits, exatamente a fronteira em que a migração pós-quântica se torna urgente, e a razão de RSA-2048 ser o cartaz do Shor.

Daqui se extrai a tese que organiza o artigo. *Aceleradores — ASIC, FPGA, energia, paralelismo — deslocam a curva de custo para baixo por um fator constante, mas não alteram sua inclinação. E a inclinação é a classe de complexidade.* Logo, nenhum acelerador muda o regime em que se está. As únicas alavancas que mudam a inclinação são duas: trocar de *classe de método* — rho (exponencial) → ECM ($\alpha = \frac{1}{2}$) → GNFS ($\alpha = \frac{1}{3}$) — ou o salto quântico (subexponencial → polinomial). Não se acelera o relógio; muda-se a geometria do tempo.

A honestidade que dá credibilidade ao levantamento: nada das Seções II–VIII é original deste autor. É o mapa público do campo — Dickman, Pomerance, Pollard, os Lenstra, Montgomery, Murphy, Kleinjung, Coppersmith, Howgrave-Graham, Heninger, Shor, Regev, Gidney — desenhado numa base consistente. O valor da síntese é diagnóstico e arquitetural, não inventivo. A invenção, se houver, mora adiante.

IX. A fronteira viva: transição pós-quântica e soberania criptográfica

Se Shor rebaixa a inclinação ao chão polinomial, então toda a criptografia de chave pública baseada em fatoração e logaritmo discreto — RSA, Diffie–Hellman, curvas elípticas — tem prazo de validade atrelado ao calendário do hardware quântico tolerante a falhas. A resposta institucional já está em curso. Em 13 de agosto de 2024, o NIST publicou os três primeiros padrões pós-quânticos finalizados: FIPS 203 (ML-KEM, derivado do CRYSTALS-Kyber) como mecanismo primário de encapsulamento de chaves; FIPS 204 (ML-DSA, derivado do CRYSTALS-Dilithium) como padrão primário de assinatura; e FIPS 205 (SLH-DSA, derivado do SPHINCS+), uma assinatura baseada em hash, concebida como método reserva caso o ML-DSA se prove vulnerável. O FALCON será publicado como FIPS 206 (FN-DSA), e o HQC foi selecionado para padronização em 11 de março de 2025 como KEM de reserva sobre base matemática distinta dos reticulados.

O imperativo de urgência tem nome: *harvest now, decrypt later*. Adversários capturam dados cifrados hoje para decifrá-los quando o hardware quântico amadurecer — de modo que qualquer informação cuja confidencialidade precise sobreviver à próxima década já está, em sentido prático, exposta. As recomendações de calendário situam a depreciação de RSA e ECC por volta de 2030 e a migração completa até 2035.

Mas há uma fragilidade estrutural na resposta atual que motiva a Seção seguinte. Dos cinco esquemas em jogo, *três* (ML-KEM, ML-DSA, FN-DSA) repousam sobre a mesma família matemática — problemas de reticulado (LWE, SIS e variantes). A concentração é compreensível (reticulados oferecem o melhor equilíbrio desempenho-segurança),

mas é um risco sistêmico: um avanço criptanalítico contra reticulados — clássico ou quântico — comprometeria simultaneamente a espinha dorsal do novo arcabouço. O SPHINCS+, baseado em hash, é o seguro de vida precisamente por ser *estruturalmente distinto*. A doutrina de soberania criptográfica que defendemos é a generalização desse princípio: não basta migrar; é preciso *diversificar* sobre fundamentos matemáticos independentes, de modo que nenhum único progresso teórico colapse o conjunto. É essa exigência — por uma primitiva genuinamente distinta, não uma quarta variação sobre reticulados — que abre o espaço para a aposta original deste artigo.

X. A inovação pura: funções mock theta como primitiva criptográfica

Tudo o que veio antes foi domínio. O que segue é a aposta de invenção — demarcada com cuidado, porque a integridade exige separar o que se domina do que se descobre, e porque mesmo aqui a parte matematicamente sólida (a teoria das mock theta) deve ser distinguida da parte conjectural (seu uso criptográfico).

X.1 A última carta de Ramanujan

Em 12 de janeiro de 1920, três meses antes de morrer aos trinta e dois anos, Srinivasa Ramanujan escreveu a G. H. Hardy a carta que se tornaria o último de seus enigmas e o primeiro de um campo inteiro. Nela, introduziu o que chamou de *mock theta functions* — "funções theta falsas" — e ofereceu dezessete exemplos, agrupados pelo que denominou, de modo informal, "ordens" 3, 5 e 7. O protótipo de ordem 3 é a série

$$f(q) = \sum_{n=0}^{\infty} \frac{q^{n^2}}{(1+q)^2(1+q^2)^2 \cdots (1+q^n)^2} = \sum_{n \geq 0} \frac{q^{n^2}}{(-q;q)_n^2},$$

onde $(-q;q)_n$ é o símbolo de q-Pochhammer. O enigma que Ramanujan colocou era de natureza analítica e profundíssima. As funções theta clássicas de Jacobi são *modulares*: transformam-se de modo controlado sob o grupo modular, e perto de cada raiz da unidade ζ exibem singularidades exponenciais precisas. Ramanujan observou que $f(q)$ *imita* esse comportamento — perto de cada raiz da unidade, comporta-se como uma theta genuína a menos de uma correção limitada — e perguntou se uma função com tal comportamento em *todas* as raízes da unidade teria necessariamente de ser a soma de uma função modular e de uma função "boa" (limitada) em todos esses pontos. Sua conjectura, correta, era que **não**: as mock theta são genuinamente novas, theta-símiles que escapam à modularidade.

X.2 Sete décadas de meio-entendimento

O enigma resistiu. G. N. Watson, num discurso presidencial à London Mathematical Society de 1936 que intitulou, com humor sombrio, "The final problem: an account of the mock theta functions", estabeleceu leis de transformação para as funções de ordem 3 e parte das de ordem 5, e demonstrou que $f(q)$ não é modular. Atle Selberg trabalhou as ordens 5 e 7. Mas o estatuto estrutural — *o que são*, a que teoria pertencem — permaneceu obscuro por mais de meio século.

O segundo marco foram as *mock theta conjectures*: um conjunto de dez identidades, registradas por Ramanujan no "lost notebook" redescoberto por George Andrews em 1976, que relacionavam as funções de ordem 5 a geradoras de tipo Hecke ligadas ao *rank* de partições de Freeman Dyson. George Andrews e Frank Garvan reduziram as dez a um par; e Dean Hickerson, num trabalho notável de 1988, "A proof of the mock theta conjectures", as demonstrou por completo. Andrews e Hickerson trataram a ordem 7. Tinha-se, ao fim dos anos oitenta, prova — mas ainda não *compreensão*.

X.3 Zwegers e a forma de Maass: a teoria revelada

A compreensão veio em 2002, na tese de doutorado de Sander Zwegers em Utrecht, orientada por Don Zagier. Zwegers mostrou o que Ramanujan intuíra sem poder formular: as funções mock theta são as **partes holomorfas de formas de Maass harmônicas fracas de peso** $1/2$. A construção é precisa e bela. Uma forma de Maass harmônica $\widehat{H}$ decompõe-se em

$$\widehat{H}(\tau) = H(\tau) + H^{-}(\tau),$$

onde H é a parte holomorfa (a mock theta propriamente dita, com τ no semiplano superior e $q = e^{2\pi i \tau}$) e H^{-} é uma parte não-holomorfa dada por um integral de período (de Eichler) de uma forma theta unária de peso $3/2$ — objeto a que Zagier deu o nome de **shadow** (sombra) da mock theta. O operador hiperbólico $\xi_{1/2} = 2iy^{1/2}\,\overline{\partial_{\bar{\tau}}}$ aplica $\widehat{H}$ exatamente sobre a sombra. É a sombra, e a obrigação de completá-la para restaurar a modularidade, que mede o quanto a função "falha" em ser theta — e que, completada, a faz transformar-se corretamente sob o grupo modular.

Esse enquadramento converteu um zoológico de curiosidades numa teoria viva. Kathrin Bringmann e Ken Ono usaram-no para demonstrar a conjectura de Andrews–Dragonette sobre as assintóticas dos coeficientes de $f(q)$ — que são, a menos de sinal, a diferença $N_e(n) - N_o(n)$ entre partições de n de rank par e ímpar — e para estabelecer congruências para o rank de Dyson. Zagier (2010) reinterpretou as mock theta como **formas modulares quânticas**, objetos definidos sobre os racionais com uma quase-modularidade de natureza nova. E a física teórica encontrou-as de modo independente: Atish Dabholkar, Sameer Murthy e Zagier mostraram que formas mock modulares contam degenerescências de buracos negros quânticos sob *wall-crossing*, e o *Mathieu moonshine* de Eguchi–Ooguri–Tachikawa exibe uma forma mock modular no caráter de uma teoria de campos superconforme. As mock theta deixaram de ser um enigma terminal de Ramanujan para se tornar um nó central entre teoria dos números, formas automorfas e teoria de cordas.

X.4 A proposta Θ-Crypt: não-identificabilidade como princípio de segurança

A aposta criptográfica deste programa — Θ-Crypt — parte de uma observação estrutural sobre a teoria da Seção X.3, e não de uma analogia frouxa. A criptografia de chave pública padrão funda-se em *dureza computacional*: fatorar, calcular logaritmos discretos, encontrar vetores curtos. A proposta aqui é deslocar o fundamento para um princípio distinto, que chamamos de **não-identificabilidade** (Axioma de Determinação Única, ADU): a dificuldade não de *inverter* uma função, mas de

determinar univocamente qual, dentre uma família estruturalmente ambígua de objetos, gerou uma observação dada.

A intuição é a seguinte. A correspondência mock theta ↔ forma de Maass harmônica ↔ sombra encerra graus de liberdade que não são recuperáveis a partir de dados parciais da q-expansão holomorfa isoladamente: a completação não-holomorfa, o emparelhamento com a sombra de peso 3/2, e a escolha dentro da família de ordens 3/5/7 (a tríade de Ramanujan–Watson–Hickerson) constituem um espaço de parâmetros cujo colapso a uma instância única, a partir de informação holomorfa truncada, é o que se postula ser intratável. Em vez de "achar o vetor curto", o adversário enfrentaria "decidir qual completação modular consistente gerou esta série" — um problema de identificação, não de inversão. As primitivas projetadas sob esse princípio (um problema de decisão MT-Decision, e análogos estruturais MT-LWE e MT-SIS que importam a geometria de erro e a sombra para o ambiente de reticulado) buscariam segurança não da ausência de algoritmo eficiente de inversão, mas da degenerescência informacional da identificação.

O atrativo de soberania é direto: se a segurança não se reduz à dureza de reticulado, então uma primitiva mock theta seria *estruturalmente independente* da família que domina o arcabouço NIST — precisamente o tipo de diversificação que a Seção IX argumentou ser necessária. Seria um candidato a "Regime III", uma alternativa cuja quebra exigiria um avanço ortogonal ao que ameaçaria os reticulados.

X.5 A fronteira honesta: o que está provado, o que está em aberto

Aqui a honestidade não é cortesia; é a substância da credibilidade científica, e este autor a prefere ao consolo. **A teoria matemática das mock theta (X.1–X.3) é sólida, demonstrada e canônica.** A *proposta criptográfica* (X.4) é, neste momento, um programa de pesquisa em estágio inicial, e três qualificações devem ser registradas sem atenuação.

Primeiro, **as reduções de segurança estão em aberto.** Não existe, até esta data, uma redução demonstrada que ligue a quebra de MT-LWE, MT-SIS ou MT-Decision a um problema reconhecidamente difícil — nem clássico, nem quântico. A não-identificabilidade é, por ora, um *princípio* heurístico de design, não um teorema de segurança. Afirmá-la como segura seria repetir o erro categórico que este artigo combateu em toda a Parte clássica: confundir a ausência de um ataque conhecido com a prova de sua inexistência.

Segundo, e como consequência direta, **o modo MT-puro é proibido em produção.** A postura responsável e mandatória do programa Θ-Crypt é estritamente *híbrida*: qualquer instância operacional combina a primitiva mock theta com um esquema padrão já validado (um ML-KEM ou um SLH-DSA), de modo que a segurança do conjunto nunca seja inferior à do componente bem-entendido. A mock theta entra como *camada de diversificação estrutural*, jamais como ponto único de confiança. Esta é a tradução de engenharia do reconhecimento de que a novidade é, hoje, conceitual e não demonstrada.

Terceiro, **o caminho à frente é a criptanálise externa adversarial.** Uma primitiva só ganha confiança sobrevivendo ao ataque de quem deseja quebrá-la; o destino natural deste programa é a publicação aberta (no padrão IACR ePrint) e o escrutínio por grupos de criptanálise de reticulados e de teoria dos números computacional de primeira linha. Maturidade tecnológica em TRL 3–4, não mais; e a honestidade sobre essa posição é o que separa um programa sério de uma promessa inflada.

A aposta, portanto, é assimétrica e deliberada: alta probabilidade de que reduções e criptanálise revelem fragilidades a corrigir, contra a pequena mas real possibilidade de que a não-identificabilidade ancorada na estrutura de Zwegers constitua um fundamento genuinamente novo — a única classe de risco que vale a pena correr, porque é a única em que a recompensa é invenção, e não mera maestria.

XI. Conclusão: a única defesa durável é estrutural

O percurso deste artigo desenha uma única figura. A fatoração de inteiros é uma paisagem de quatro regimes, e cada um é uma geometria de custo: a parede exponencial de Pollard, o arco subexponencial de Lenstra e do crivo, o piso polinomial de Shor. A lei que governa a paisagem é que o hardware desloca a curva por um fator constante, mas só a mudança de classe matemática — ou o salto quântico — altera sua inclinação. Disso decorre o diagnóstico de longo prazo: contra um adversário clássico, a engenharia compra fatores constantes valiosos dentro da mesma curva; contra um adversário quântico tolerante a falhas, a curva inteira cede, e nenhuma quantidade de silício clássico a defende.

Por isso a defesa durável não pode ser quantitativa — mais bits, mais núcleos, chaves maiores. Ela tem de ser *qualitativa e estrutural*: fundar a confiança em problemas matemáticos diversos e independentes, de modo que nenhum avanço único colapse o conjunto. O arcabouço pós-quântico atual, concentrado em reticulados, é um começo necessário mas insuficientemente diversificado. A aposta nas funções mock theta — o tesouro que Ramanujan deixou em sua última carta, decifrado por Zwegers oitenta anos depois — é uma tentativa de oferecer essa independência estrutural: uma primitiva cuja segurança, *se* vier a ser estabelecida, repousaria não sobre a dureza de inverter, mas sobre a impossibilidade de identificar. Que essa segurança permaneça por demonstrar não é uma fraqueza a esconder; é a fronteira exata onde a invenção, e não o domínio, está em jogo.

Apêndice A — Formalização dos problemas MT-*

Este apêndice enuncia, com precisão, os três problemas cuja dureza *conjectural* fundamentaria o arcabouço Θ-Crypt. Eles são apresentados para **escrutínio criptanalítico**, e não como problemas reconhecidamente difíceis: o panorama de reduções (A.5) está, em sua quase totalidade, em aberto, e a superfície de ataque (A.6) é apresentada como a agenda de falsificação que deve preceder qualquer afirmação de segurança. A notação segue Zwegers (2002) e Bringmann–Folsom–Ono–Rolen no lado automorfo, e o gabarito LWE/SIS de Ajtai e Regev no lado de reticulados.

A.1 O objeto estruturado: forma de Maass harmônica, sombra, e o reticulado de coeficientes

Fixe a ordem $\omega \in \{3,5,7\}$, um nível N_ω e um sistema multiplicador. Seja $\mathcal{M}_\omega$ o espaço (de dimensão finita) das formas de Maass harmônicas fracas de peso $1/2$ cujas partes holomorfas são funções mock theta de ordem ω. Para $\widehat{H} \in \mathcal{M}_\omega$, escreva $\widehat{H} = H + H^-$, com parte holomorfa $H(\tau) = \sum_{n \gg -\infty} a(n)\, q^n$ ($q = e^{2\pi i \tau}$) e **sombra** $g = \xi_{1/2}\big(\widehat{H}\big)$, uma forma theta unária cuspidal de peso $3/2$,

$$g(\tau) = \sum_{n \in \mathbb{Z}} n\ \chi(n)\, q^{\,n^2/(4N_\omega)},$$

atrelada a uma forma quadrática e a um caráter χ. Três fatos estruturais são explorados:

(i) a completação H^- é o integral de período (de Eichler) da sombra conjugada,

$$H^-(\tau) = C_\omega \int_{-\bar{\tau}}^{i\infty} \frac{\overline{g(-\bar{z})}}{(z+\tau)^{1/2}}\, dz,$$

de modo que a parte não-holomorfa é **inteiramente determinada** por g;

(ii) o operador $\xi_{1/2}\colon \mathcal{M}_\omega \to S_{3/2}$ é sobrejetor sobre o espaço relevante de theta de peso $3/2$, com núcleo de dimensão finita (as formas genuinamente modulares de peso $1/2$) — a sombra é "quase" um invariante completo, a menos desse núcleo;

(iii) os coeficientes $a(n)$ obedecem assintóticas do tipo Andrews–Dragonette–Rademacher,

$$a(n) \sim \frac{(-1)^{n-1}}{2\sqrt{n}} \exp\left(\pi\sqrt{n/6}\right) \cdot \big(1 + o(1)\big),$$

com fina estrutura aritmética (geradoras de *rank* de partições). É essa combinação — crescimento subexponencial previsível na escala grosseira, porém com flutuação aritmética fina — que faz vetores de coeficientes truncados *parecerem* pseudoaleatórios módulo um primo q enquanto secretamente repousam sobre um reticulado estruturado.

Defina, para um truncamento D e módulo q, o **mapa de coeficientes** $\varphi_D\colon \mathcal{M}_\omega \to \mathbb{Z}_q^D$, $\widehat{H} \mapsto \big(a(1), \dots, a(D)\big) \bmod q$ — isto é, *apenas* a parte holomorfa, o dado publicamente observável. O **reticulado mock-modular** $\Lambda_\omega^{(D)}$ é o conjunto dos vetores inteiros de coeficientes que se estendem a uma forma harmônica consistente (que *admitem* uma sombra), uma estrutura (sub)reticular de $\mathbb{Z}^D$ de posto ligado a $\dim\mathcal{M}_\omega$. O **princípio de não-identificabilidade (ADU)** é a asserção de que, a partir de $\varphi_D\big(\widehat{H}\big)$ apenas, com D limitado, a completação — logo a sombra g, logo $\widehat{H}$ e qualquer segredo nela codificado — não é unívoca nem eficientemente recuperável.

A.2 MT-SIS (Mock-Theta Short Integer Solution)

Recorde o SIS de Ajtai: dada $A \in \mathbb{Z}_q^{n\times m}$ uniforme, achar $z \in \mathbb{Z}^m$, $0 < \| z \| \leq \beta$, com $Az \equiv 0$. O MT-SIS substitui a matriz uniforme pelos vetores de coeficientes de uma base mock theta.

> **Problema (MT-SIS$_{\omega,q,D,k,\beta}$).** Dada uma base $\{\widehat{H}_1, \dots, \widehat{H}_k\} \subset \mathcal{M}_\omega$ e seus vetores $\varphi_D(\widehat{H}_i) \in \mathbb{Z}_q^D$, encontrar $z \in \mathbb{Z}^k$ com $0 < \| z \| \leq \beta$ tal que
>
> $$\sum_{i=1}^{k} z_i \ \varphi_D(\widehat{H}_i) \equiv 0 \pmod{q},$$
>
> ou seja, uma combinação **curta** de mock theta cujas partes holomorfas se cancelam módulo q até a ordem D.

Intuição da dureza conjectural. Uma relação curta entre coeficientes truncados é um vetor curto em $\Lambda_\omega^{(D)}$; a pseudoaleatoriedade de A.1(iii) deveria fazer o reticulado comportar-se como um reticulado q-ário aleatório, para o qual achar vetores curtos é SVP-difícil no pior caso. Mas $\Lambda_\omega^{(D)}$ **não** é aleatório: carrega estrutura modular e de Hecke, e se essa estrutura abre um atalho é exatamente a questão em aberto. *Status:* nenhuma redução pior-caso–caso-médio conhecida.

A.3 MT-LWE (Mock-Theta Learning With Errors), com erro estruturado pela sombra

Recorde o LWE de Regev: $(A,\ b = As + e)$, e Gaussiano discreto; recuperar s (busca) ou distinguir de uniforme (decisão). No MT-LWE o **erro é a completação não-holomorfa** — o ruído carrega a sombra.

> **Problema (MT-LWE$_{\omega,q,D,\chi}$, busca).** Seja $s \in \mathbb{Z}_q^k$ secreto. Para $i = 1, \dots, m$, amostre $\widehat{H}^{(i)} \in \mathcal{M}_\omega$ e publique
>
> $$\left(\varphi_D(\widehat{H}^{(i)}),\ \ b_i = \langle s,\ \varphi_D(\widehat{H}^{(i)})\rangle + e_i \bmod q\right),$$
>
> onde $e_i \leftarrow \chi_g$, distribuição sobre $\mathbb{Z}_q$ cuja covariância é ditada pelos coeficientes do integral de período da sombra $g^{(i)}$ de $\widehat{H}^{(i)}$ — um Gaussiano discreto *deformado pela parte não-holomorfa*. Recuperar s.
>
> **Decisão.** Distinguir $\{(\varphi_D(\widehat{H}^{(i)}),\ b_i)\}$ de $\{(\varphi_D(\widehat{H}^{(i)}),\ u_i)\}$ com u_i uniforme.

O papel do ADU. Como o erro É a sombra, um adversário capaz de *destacar* a completação — identificar a cisão holomorfo/não-holomorfo a partir do dado truncado — reduziria o MT-LWE à álgebra linear trivial. A conjectura é que esse destacamento é precisamente o passo não-identificável. Em contraste, a parte legítima detém a completação (a *trapdoor* é o conhecimento da sombra e dos parâmetros) e inverte em tempo polinomial. *Status:* a equivalência busca–decisão e qualquer redução ao LWE/reticulados padrão estão em aberto; se χ_g é "bem-espalhada" o bastante, ou se sua estrutura de sombra vaza, é o alvo criptanalítico central.

A.4 MT-Decision: a versão computacional da pergunta de Ramanujan (1920)

O mais conceitualmente puro dos três, e o que fecha o arco histórico do artigo.

> **Problema (MT-Decision$_{\omega,q,D}$).** Dado $v \in \mathbb{Z}_q^D$, decidir entre: **(a)** $v = \varphi_D(\widehat{H})$ para alguma $\widehat{H} \in \mathcal{M}_\omega$ — isto é, v admite uma completação modular consistente (uma sombra); **(b)** v é *theta-símile espúrio* — reproduz o comportamento theta até a ordem D sem ser a parte holomorfa de nenhuma forma harmônica de peso $1/2$ (nenhuma sombra consistente existe).

Esta é, literalmente, a forma decisional-computacional da pergunta que Ramanujan colocou a Hardy em 1920: *o comportamento theta-símile até ordem limitada força a (mock)modularidade genuína?* A conjectura é que, para parâmetros adequados, decidir a consistência a partir de dado truncado é intratável — um engodo pode ser feito theta-símile até a ordem D e ainda assim não-completável, e separá-los é o gargalo do ADU. É este problema de distinção que fundamentaria a segurança IND-CPA de um KEM. *Status:* em aberto; a redução MT-Decision ≤ MT-LWE (decisão) é plausível, porém não demonstrada.

A.5 O panorama de reduções: o que se quer provar, e o que está aberto

A honestidade exige tabular o que *faltaria* demonstrar. Praticamente tudo:

1. **Pior-caso → caso-médio** (estilo Ajtai para MT-SIS; estilo Regev para MT-LWE), ancorando a dureza média num problema de reticulado de pior caso — **inexistente**.
2. **Equivalência busca–decisão** para MT-LWE — **inexistente**.
3. **Reduções inter-problemas** (MT-SIS ↔ MT-LWE ↔ MT-Decision) — **conjecturais**.
4. **O teorema de composição híbrida.** Que um esquema combinando a primitiva mock theta P_{MT} com uma primitiva padronizada P_{std} (e.g., ML-KEM) num *combinador de KEM* seja IND-CCA seguro se *qualquer um* dos componentes o for — **isto, e somente isto, se sustenta hoje**, e se sustenta *genericamente*, pela segurança do combinador (Giacon–Heuer–Poettering; Bindel et al.), e **não** porque MT-* seja provadamente difícil.

Aqui está o cerne honesto: o único teorema disponível é "o híbrido não é mais fraco do que sua perna padrão". Tudo o que faria a perna mock theta *contribuir* com segurança está em aberto — e é exatamente por isso que o modo MT-puro é proibido: a prova do híbrido repousa inteiramente sobre P_{std} até que, e a menos que, as reduções MT-* existam.

A.6 Superfície de ataque: o que um criptanalista deveria tentar primeiro

A lista a seguir é, simultaneamente, a superfície de ataque e a agenda de pesquisa — os testes de falsificação que o programa precisa sobreviver antes de qualquer reivindicação:

- **Redução de reticulado** (LLL/BKZ) diretamente sobre $\Lambda_{\omega}^{(D)}$ / o reticulado q-ário de coeficientes; estimar o *gap* e o bloco BKZ necessário.
- **Predição de coeficientes** via as fórmulas exatas de Hardy–Ramanujan–Rademacher e Andrews–Dragonette: *este é o ataque mais perigoso*. Se $a(n)$ for previsível com precisão suficiente, a pseudoaleatoriedade de φ_D colapsa e o segredo (ou o engodo) fica exposto. Quantificar a precisão atingível é pré-requisito de qualquer segurança.
- **Operadores de Hecke**: a ação de Hecke sobre os coeficientes produz relações lineares que poderiam encurtar o MT-SIS ou destacar a sombra no MT-LWE.
- **Recuperação direta de sombra**: qualquer método subexponencial para reconstruir g a partir de $a(n)$ truncado quebra o ADU na raiz.
- **Estrutura de χ_g**: vazamento por canal lateral ou viés estatístico na distribuição de erro do MT-LWE.

O valor do programa está precisamente em que esses testes são **concretos** e que a sobrevivência a eles — sobretudo ao ataque de predição de Andrews–Dragonette — é *necessária* antes de qualquer afirmação de segurança. Até lá, a posição é a que o corpo do artigo declarou: maturidade TRL 3–4, e uso exclusivamente híbrido.

Referências seminais

Teoria analítica e fatoração. K. Dickman, *On the frequency of numbers containing prime factors of a certain relative magnitude* (1930). C. Pomerance, *Analysis and comparison of some integer factoring algorithms* (1982); *The quadratic sieve factoring algorithm* (1985). E. R. Canfield, P. Erdős, C. Pomerance, *On a problem of Oppenheim concerning "factorisatio numerorum"* (1983). R. Crandall, C. Pomerance, *Prime Numbers: A Computational Perspective* (2005). G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory*.

Métodos de ordem fixa e crivo. J. M. Pollard, *Theorems on factorization and primality testing* (1974); *A Monte Carlo method for factorization* (1975). A. K. Lenstra, H. W. Lenstra Jr. (eds.), *The Development of the Number Field Sieve*, LNM 1554 (1993). B. Murphy, *Polynomial Selection for the Number Field Sieve Integer Factorisation Algorithm*, tese, ANU (1999). H. Cohen, *A Course in Computational Algebraic Number Theory*, GTM 138.

Curvas elípticas. H. W. Lenstra Jr., *Factoring integers with elliptic curves* (1987). P. L. Montgomery, *Speeding the Pollard and elliptic curve methods of factorization* (1987). D. J. Bernstein, P. Birkner, T. Lange, C. Peters, *ECM using Edwards curves* (2008). J. H. Silverman, *The Arithmetic of Elliptic Curves*, GTM 106.

Reticulados e informação parcial. A. K. Lenstra, H. W. Lenstra Jr., L. Lovász, *Factoring polynomials with rational coefficients* (1982). D. Coppersmith, *Small solutions to polynomial equations, and low exponent RSA vulnerabilities* (1997). N. Howgrave-Graham, *Finding small roots of univariate modular equations revisited*

(1997). N. Heninger, H. Shacham, *Reconstructing RSA private keys from random key bits* (2009). S. Galbraith, *Mathematics of Public Key Cryptography*.

Regime quântico. P. W. Shor, *Algorithms for quantum computation: discrete logarithms and factoring* (1994). C. Gidney, M. Ekerå, *How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits* (2019). C. Gidney, *How to factor 2048 bit RSA integers with less than a million noisy qubits*, arXiv:2505.15917 (2025). O. Regev, *An efficient quantum factoring algorithm* (2023). M. A. Nielsen, I. L. Chuang, *Quantum Computation and Quantum Information*.

Padronização pós-quântica. NIST, FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), FIPS 205 (SLH-DSA), 13 ago. 2024; HQC selecionado em 11 mar. 2025; FN-DSA (FIPS 206) em desenvolvimento.

Funções mock theta. S. Ramanujan, última carta a G. H. Hardy (12 jan. 1920); *The Lost Notebook and Other Unpublished Papers*. G. N. Watson, *The final problem: an account of the mock theta functions* (1936). D. Hickerson, *A proof of the mock theta conjectures* (1988). G. E. Andrews, D. Hickerson, *Ramanujan's "lost" notebook VII: the sixth order mock theta functions* (1991). S. P. Zwegers, *Mock Theta Functions*, tese de doutorado, Universiteit Utrecht (2002). K. Bringmann, K. Ono, *The $f(q)$ mock theta function conjecture and partition ranks* (2006). D. Zagier, *Quantum modular forms* (2010). A. Dabholkar, S. Murthy, D. Zagier, *Quantum Black Holes, Wall Crossing, and Mock Modular Forms*.

Reduções, reticulados e formas modulares (Apêndice A). M. Ajtai, *Generating hard instances of lattice problems* (1996). O. Regev, *On lattices, learning with errors, random linear codes, and cryptography* (2005). D. Micciancio, O. Regev, *Worst-case to average-case reductions based on Gaussian measures* (2007). C. Gentry, C. Peikert, V. Vaikuntanathan, *Trapdoors for hard lattices and new cryptographic constructions* (2008). V. Lyubashevsky, C. Peikert, O. Regev, *On ideal lattices and learning with errors over rings* (2010). F. Giacon, F. Heuer, B. Poettering, *KEM combiners* (2018); N. Bindel, J. Brendel, M. Fischlin, B. Goncalves, D. Stebila, *Hybrid key encapsulation mechanisms and authenticated key exchange* (2019). K. Bringmann, A. Folsom, K. Ono, L. Rolen, *Harmonic Maass Forms and Mock Modular Forms: Theory and Applications* (AMS Colloquium, 2017).