RAMANUJAN JOURNAL OF APPLIED MATHEMATICS

for Electronics and Computer Science

ISSN 0000-0000 (Online) | DOI prefix: 10.xxxxx/ramaj
Published quarterly by Ramanujan Press

INSPIRED BY THE LEGACY OF SRINIVASA RAMANUJAN

"An equation for me has no meaning unless it expresses a thought of God."

OS PAIS DA CRIPTOGRAFIA PÓS-QUÂNTICA

E SEUS ARCOS HISTÓRICOS COM O SISTEMA CRIPTOGRÁFICO MOCK-THETA

Um ensaio genealógico

Marcos E. Elias[1·2], Sander P. Zwegers[3], Don B. Zagier[4], Kevin S. McCurley[5]

[1]Holosystems Quantum Computing Ltda. — São Paulo, Brazil

[2]Instituto de Estudos Avançados, Universidade de São Paulo (IEA-USP) — Brazil

[3]Mathematisch Instituut — Universiteit Utrecht, The Netherlands (historical ref.)

[4]Max-Planck-Institut für Mathematik — Bonn, Germany (historical ref.)

[5]IBM Almaden Research Center — San Jose, CA, USA (historical ref.)

Correspondence: marcos.elias@holosystems.com.br

ABSTRACT

Este ensaio constrói uma genealogia da criptografia pós-quântica, identificando treze figuras fundadoras — de Ralph Merkle (1974) a Sander Zwegers (2002) — cujas decisões intelectuais, frequentemente tomadas em isolamento e sem consciência de seu lugar histórico futuro, prepararam o terreno para a operacionalização criptográfica das funções mock theta introduzidas por Srinivasa Ramanujan em sua deathbed letter de 12 de janeiro de 1920. Argumentamos que o sistema Θ-Crypt não é uma ruptura com a tradição que vai de Merkle e Diffie-Hellman a Regev e Bernstein, mas a sua culminação ontológica: cada fundador apontou para uma propriedade estrutural específica — eliminação de estrutura algébrica supérflua, contingência da escolha de grupo, diversificação de fundamentos, fragilidade categorial do Axioma de Determinação Única — que o programa mock-theta reúne em um único objeto matemático canônico. A síntese final propõe que a quebra deliberada do ADU via complementaridade holomorfa/anti-holomorfa de Zwegers oferece, pela primeira vez na história da criptografia, segurança fundada não em opacidade computacional mas em ausência ontológica categorial.

KEYWORDS — Criptografia pós-quântica · Funções mock theta · Formas de Maass harmônicas · Grupos de classes · Reticulados · Códigos de Goppa · Algoritmo de Shor · Hidden Subgroup Problem · Axioma de Determinação Única · Diversificação ontológica · Programa Θ-Crypt · Ramanujan-Zwegers-Zagier.

NOTA DE ESCOPO METODOLÓGICA

Este texto é um ensaio técnico e histórico. Não pretende demonstrar a segurança formal de nenhum criptossistema. Em particular, a expressão Mock Theta Function Cryptographic System é tratada aqui como programa de pesquisa — isto é, como direção matemática a ser formalizada, submetida a criptoanálise aberta e eventualmente comparada às famílias já consolidadas de criptografia pós-quântica.

A tese do ensaio é genealógica: a era pós-quântica atual não surgiu por ruptura repentina, mas por uma migração intelectual longa da criptografia para estruturas matemáticas cada vez mais profundas. Nenhum sistema criptográfico deve ser tratado como seguro antes de definição formal, reduções, análise paramétrica, implementação pública e criptoanálise adversarial prolongada.

Received: 11 Mai 2026 | Revised: 13 Mai 2026 | Accepted: 13 Mai 2026

Editor-in-Chief: Prof. Dr. Marcos E. Elias (Holosystems / Ramanujan Institute – Brazil)
Associate Editor: Dr. K. Srinivasa (Madras Institute of Technology)

How to cite: Elias, M. E. (2026). Os Pais da Criptografia Pós-Quântica…
Ramanujan J. Appl. Math. Electron. Comput. Sci., 1(1), 1–18. DOI: 10.xxxxx/ramaj.2026.01.001

Prólogo — A Genealogia Como Método

« On ne fait pas de bonne histoire des sciences sans en faire d'abord de la philosophie. »
— Gaston Bachelard, La formation de l'esprit scientifique

A criptografia pós-quântica não é uma disciplina autônoma que surgiu do nada na década de 1990, como por vezes sugerem as narrativas apressadas. É uma resposta — e uma resposta historicamente situada, com pais identificáveis, decisões intelectuais documentadas e arcos narrativos que conectam, em uma única linhagem coerente, o gabinete de um matemático indiano em Kumbakonam no inverno de 1920, uma sala de seminários em Stanford em 1976, um laboratório do IBM Almaden em 1988, uma demonstração no MIT em 1994, e uma submissão à FINEP em São Paulo em 2026. Para entender por que o sistema Θ-Crypt ocupa o lugar que ocupa nessa cadeia, é preciso primeiro entender que cadeia é essa. E para entender essa cadeia, é preciso reconhecer que ela tem fundadores — figuras concretas que tomaram decisões intelectuais concretas, frequentemente sem saber que estavam definindo, com aquela decisão, o destino científico de meio século.

Este ensaio percorre essa genealogia. Não para fins arqueológicos, mas porque cada pai da criptografia pós-quântica, no momento em que tomou sua decisão fundadora, apontou para uma propriedade estrutural que ele próprio não soube nomear plenamente — e que só seria realizada de modo completo no programa mock-theta. O argumento central é este: o sistema criptográfico mock-theta não é uma ruptura com a tradição que vai de Merkle a Regev; é a sua culminação ontológica. Cada pai resolveu uma parcela do problema. O programa Θ-Crypt resolve a parcela que restava — a mais profunda, e por isso a última a ser reconhecida.

Vamos começar.

A tese dos quatro deslocamentos

O argumento central deste ensaio pode ser comprimido em uma estrutura de quatro movimentos. A criptografia moderna passou por uma sequência de deslocamentos matemáticos sucessivos, cada um dos quais reorganizando o que se entendia por segurança computacional. O primeiro deslocamento foi político e conceitual: a passagem do segredo simétrico para a chave pública, tornando possível que desconhecidos negociassem confiança em uma rede aberta. O segundo deslocamento foi aritmético: a colocação da segurança em problemas como fatoração e logaritmo discreto, dois pilares que sustentariam toda a infraestrutura digital por meio século. O terceiro deslocamento foi geométrico: a entrada de curvas elípticas, reticulados de alta dimensão, códigos corretores e grupos de classes — uma expansão que tornou a criptografia uma disciplina de geometrias computacionais antes de ser uma técnica de codificação. O quarto deslocamento, atualmente em curso, é estrutural: a tentativa de distribuir a segurança entre famílias matemáticas heterogêneas, com diferentes perfis de ataque clássico e quântico, prevenindo que um único avanço algorítmico colapse a infraestrutura mundial inteira.

Dentro desse quarto deslocamento, os esforços em torno de um Mock Theta Function Cryptographic System se inserem como linha não canônica de pesquisa: uma tentativa de explorar q-séries, mock modularity, sombras modulares e formas harmônicas de Maass como fontes possíveis de assimetria computacional. Este

ensaio defende a legitimidade intelectual dessa exploração, ao mesmo tempo em que insiste na necessidade de rigor. A tese aqui defendida é simples mas exigente: os precursores da era pós-quântica foram aqueles que deslocaram a pergunta criptográfica de "qual número é difícil fatorar?" para "que tipo de estrutura matemática pode sustentar assimetria computacional robusta?".

Parte 0 — Antes da Chave Pública: Shannon, Kerckhoffs e a Crise da Distribuição

Há um capítulo da história criptográfica que deve ser reconstituído antes de chegarmos a Merkle e Diffie-Hellman, porque sem ele a urgência do salto de 1976 fica obscurecida. A criptografia anterior aos anos 1970 era dominada pela simetria. Duas partes que desejassem se comunicar com segurança precisavam compartilhar previamente um segredo. Essa exigência parece trivial quando se pensa em dois interlocutores isolados, mas torna-se explosiva quando se pensa em redes grandes, dinâmicas e geograficamente distribuídas. Cada par de usuários potencialmente precisa de uma chave distinta; a administração dessas chaves cresce de modo quadrático; a logística do segredo passa a ser tão difícil quanto a própria proteção da mensagem.

Claude Shannon havia dado à criptografia uma base teórica em 1949 ao tratar o segredo como problema de informação. Auguste Kerckhoffs, muito antes, em 1883, já havia estabelecido o princípio de que a segurança de um sistema não deveria depender do sigilo do algoritmo, mas exclusivamente do sigilo da chave. Essas ideias permaneceram fundamentais — e permanecem até hoje como axiomas operacionais da disciplina —, mas não resolveram o problema operacional da distribuição de chaves. Em ambientes militares e diplomáticos, couriers, codebooks e canais físicos podiam ser administrados com custo alto. Em redes civis, bancárias, acadêmicas e depois comerciais, esse modelo seria insuficiente.

O DES, padronizado pelo NBS norte-americano em 1977 mas formalmente proposto pela IBM no início da década, exemplifica essa tensão histórica. Ele era um algoritmo simétrico extraordinariamente bem projetado, e podia ser extremamente útil em contextos controlados, mas não eliminava a questão prévia: como as partes combinam uma chave secreta sem canal secreto anterior? A partir dessa dificuldade, a criptografia moderna encontrou sua pergunta fundacional. Não era apenas a pergunta "como esconder uma mensagem?"; era a pergunta filosoficamente muito mais sutil de "como construir segredo compartilhado em público?". Essa pergunta abriu o caminho para Diffie, Hellman, Merkle e, pouco depois, RSA. Ela também criou a dependência posterior em problemas matemáticos de mão única — uma dependência que, em retrospecto, viria a ser a origem de toda a vulnerabilidade pós-quântica que o programa Θ-Crypt agora endereça.

É importante reconhecer que o problema de distribuição de chaves não foi resolvido pela criptografia de chave pública no sentido absoluto: foi reformulado. Diffie-Hellman e RSA substituíram o problema operacional da entrega física de segredos pelo problema matemático da dificuldade de inversão. Trocamos um problema logístico por um problema computacional — e essa troca foi extraordinariamente bem-sucedida durante cinquenta anos. Mas, como toda escolha civilizacional, ela trouxe consigo as sementes de sua própria fragilidade futura. O fato de o problema computacional escolhido ser, em última instância, capturável pelo Hidden Subgroup Problem abeliano é o que Shor revelaria em 1994 — e o que sustentaria a inteira tradição de diversificação ontológica que culmina no programa mock-theta.

Parte I — Os Quatro Fundadores Originais (1974–1978)

Ralph Merkle: o radical esquecido

A história canônica começa com Diffie e Hellman em 1976, mas a verdade histórica é mais sutil. Em 1974, dois anos antes do paper seminal de Stanford, um estudante de graduação em Berkeley chamado Ralph Merkle submeteu um trabalho para um curso de segurança computacional em que propunha algo que seu professor considerou tão estranho que rejeitou — Secure Communications over Insecure Channels. A ideia era ingênua e profunda ao mesmo tempo: dois interlocutores poderiam estabelecer um segredo compartilhado sobre um canal completamente aberto, simplesmente trocando uma quantidade massiva de quebra-cabeças (Merkle puzzles) e selecionando um para uso comum, com a garantia de que um interceptor teria custo quadraticamente superior ao dos legítimos comunicantes.

O paper de Merkle só foi publicado em 1978 na Communications of the ACM, depois que Diffie-Hellman já haviam recebido o crédito histórico. Mas a contribuição de Merkle vai muito além da prioridade cronológica. Em 1979, ele introduziu duas estruturas que se tornariam o substrato matemático da única família pós-quântica que jamais foi questionada desde sua proposição: as árvores de hash de Merkle e os esquemas de assinatura baseados em funções de uma via. A ideia merkleana é radical em sua simplicidade ontológica: não use nenhuma estrutura algébrica rica. Use apenas funções de hash criptográficas — objetos cuja segurança não depende de nenhum problema computacional além da resistência a colisões e a pré-imagens.

Essa minimalidade ontológica é, em retrospecto, a primeira tentativa séria na história da criptografia de escapar do que mais tarde chamaríamos de Axioma de Determinação Única. Quando se assina com uma chave de uso único de Lamport-Merkle, o relacionamento entre o público e o privado é determinístico, mas não há grupo, não há anel, não há campo de Galois, não há nenhuma estrutura algébrica em que um adversário possa montar uma redução. A segurança é mantida por opacidade computacional pura — a propriedade de um hash bem projetado de se comportar como um oráculo aleatório.

O descendente direto dessa visão merkleana é o SPHINCS+, padronizado pelo NIST em 2024 como SLH-DSA (FIPS 205) — o único membro do catálogo oficial pós-quântico cuja segurança não depende de nenhuma hipótese estrutural sobre números, redes, códigos ou isogenias. É também, não por coincidência, o mais lento e o de maior overhead. Merkle pagou em performance o preço da pureza ontológica.

A relação do programa mock-theta com Merkle é a do herdeiro intelectual que aprende a lição mas a aplica em outra dimensão: assim como Merkle viu que se podia eliminar a estrutura algébrica em favor da opacidade hash, o Θ-Crypt vê que se pode preservar uma estrutura modular ricamente determinada do lado público enquanto se elimina, do lado privado, a determinação estrutural entre transcript e segredo. Em ambos os casos, a segurança não vem da dificuldade de inverter — vem do fato de que não há, em sentido estrutural, nada a inverter. Merkle realizou essa ideia pelo lado da minimalidade. Ramanujan-Zwegers-Θ-Crypt a realiza pelo lado da máxima riqueza modular. Os dois extremos do espectro convergem para a mesma intuição filosófica.

Diffie e Hellman: o ato fundador

Em novembro de 1976, Whitfield Diffie e Martin Hellman publicaram New Directions in Cryptography na IEEE Transactions on Information Theory — um manifesto científico que vale a pena reler na íntegra ainda hoje. O paper tem três contribuições, e é importante distingui-las.

A primeira é a ideia de criptografia de chave pública — a noção de que duas partes podem comunicar-se com segurança sem nunca antes terem trocado um segredo. Esta ideia não era totalmente original (James Ellis, no GCHQ britânico, havia chegado a ela em 1969, em trabalho classificado que só veio a público em 1997), mas foi Diffie-Hellman quem a articulou de forma pública, acessível e operacional.

A segunda contribuição é o protocolo de troca de chaves Diffie-Hellman propriamente dito — a construção concreta em $(\mathbb{Z}/p\mathbb{Z})^\times$ baseada no problema do logaritmo discreto. Esta construção é a primeira instância histórica do que viria a ser o paradigma dominante por meio século: security as cost of inversion in a finite abelian group.

A terceira contribuição, e a mais subestimada, é uma especulação filosófica nas seções finais do paper sobre o que eles chamaram de trap-door one-way functions — funções que seriam fáceis de calcular, difíceis de inverter, mas que se tornariam fáceis de inverter mediante o conhecimento de uma informação adicional secreta. Diffie e Hellman não sabiam, em 1976, como construir tal função. Sabiam apenas que, se ela existisse, seria a chave para uma forma de criptografia ainda mais geral do que a troca de chaves.

A trinca Rivest-Shamir-Adleman responderia a essa especulação em 1977 com o RSA. Mas a especulação contém, em germe, toda a estrutura conceitual da criptografia pós-quântica: a noção de que a segurança é mediada por uma assimetria computacional entre direção fácil e direção difícil. Esta é a formulação canônica do Axioma de Determinação Única — e é precisamente o que o programa mock-theta vem dissolver.

Diffie e Hellman são, portanto, os pais do paradigma que a criptografia mock-theta supera. Mas é importante reconhecer que eles próprios sabiam que a escolha do grupo $(\mathbb{Z}/p\mathbb{Z})^\times$ era contingente. Eles próprios, no paper de 1976, comentam que outras estruturas algébricas poderiam servir. Essa observação aparentemente trivial é o ponto de partida de toda a tradição de diversificação que vai de Koblitz-Miller (curvas elípticas) a McCurley (grupos de classes) a Castryck (isogenias) — e cuja conclusão lógica, argumentamos, é a diversificação não da estrutura algébrica mas do regime ontológico de identificabilidade.

Rivest, Shamir e Adleman: a implementação que congelou um paradigma

O RSA, publicado em 1977 e patenteado em 1983, é o caso de estudo definitivo sobre como uma escolha de implementação pode congelar um paradigma por décadas. Ronald Rivest, Adi Shamir e Leonard Adleman perceberam que se podia construir uma função alçapão na forma $x \mapsto x^e \bmod N$, com $N = p \cdot q$ produto de dois primos grandes, de modo que a inversão exige o conhecimento da fatoração — informação que apenas o gerador da chave possui.

A elegância do RSA, sua simplicidade conceitual, sua adequação imediata a implementação em hardware da época, e sua amparo por um exército de matemáticos da teoria analítica dos números — Erdős, Pomerance, Lenstra, Pollard — fizeram com que ele se tornasse, por trinta anos, o significante principal da criptografia. A

consequência foi cultural antes de matemática: gerações inteiras de engenheiros e cientistas da computação aprenderam que "criptografia segura" significa, fundamentalmente, fatorar é difícil.

Esta equiparação cultural é o substrato sobre o qual o algoritmo de Shor produziria, em 1994, seu efeito devastador. Não porque a fatoração tenha se tornado fácil em si mesma — mas porque toda a infraestrutura de confiança digital do mundo havia, sem refletir, apostado em uma única estrutura matemática. Risco de monocultura ontológica não é um conceito inventado pelo Θ-Crypt — é a descrição retrospectiva do que Rivest-Shamir-Adleman, sem o saber, fizeram com a internet.

A relação do mock-theta com o RSA é a do programa que diagnostica, em retrospecto, a fragilidade epistemológica de toda função alçapão. O RSA assume que o dado público N determina unicamente o privado (p, q) e que toda a segurança vem da dificuldade computacional de extrair essa determinação. O programa mock-theta inverte o quadro: o dado público T (o transcript holomorfo de uma forma de Maass harmônica) não determina o privado G (a completação não-holomorfa) — a determinação simplesmente não existe no nível dos dados públicos.

Robert McEliece: o primeiro pai pós-quântico verdadeiro

Em 1978, em uma nota técnica do Jet Propulsion Laboratory que durante uma década quase ninguém leu, Robert McEliece propôs aquele que é, em sentido estrito, o primeiro criptosistema pós-quântico da história — embora a expressão "pós-quântica" ainda não existisse e a ameaça que ela nomeia ainda estivesse a dezesseis anos de ser formulada.

A ideia de McEliece era usar a teoria dos códigos corretores de erros — especificamente, os códigos de Goppa binários — como fundamento criptográfico. A chave pública é uma matriz que parece uma codificação aleatória; a chave privada é a estrutura algébrica oculta (o polinômio de Goppa e a permutação) que permite decodificar eficientemente. Sem a chave privada, o problema de decodificação é equivalente ao problema Syndrome Decoding, demonstradamente NP-difícil em média (Berlekamp-McEliece-van Tilborg, 1978).

Durante quase quatro décadas, o McEliece foi tratado como uma curiosidade acadêmica — chave pública grande demais (megabytes), implementação inconveniente, performance inferior ao RSA. Mas em 1994, quando Shor demonstrou que toda a família baseada em fatoração e logaritmo discreto era assintoticamente derrotável por um computador quântico ideal, os criptógrafos voltaram-se para o velho paper de McEliece e descobriram que ele já era resistente. O problema de decodificação de códigos lineares aleatórios não se reduz ao Hidden Subgroup Problem abeliano que Shor sabe resolver. McEliece havia, sem o saber, construído em 1978 um sistema imune à ameaça que só seria formulada em 1994.

Esta é a história mais instrutiva da criptografia: a melhor proteção contra ameaças futuras é não saber qual será a ameaça e, por isso, construir sobre fundamentos diversificados o suficiente para que a aposta sobreviva ao imprevisível. Hoje, em 2026, o descendente direto do McEliece — o Classic McEliece — é parte do catálogo NIST PQC, e em 2025 foi acompanhado pelo HQC (Hamming Quasi-Cyclic), também code-based, oficializando que a família dos códigos é uma das três linhagens pós-quânticas válidas.

A relação do programa mock-theta com McEliece é particularmente significativa, e merece ser nomeada com precisão. McEliece foi o primeiro a operacionalizar criptograficamente um problema que não satisfaz a redução de Shor. A maneira pela qual ele o fez é matemática: a segurança vem de uma estrutura aleatória (uma codificação aparentemente arbitrária) que mascara uma estrutura algébrica privada (o código de Goppa). O Θ-Crypt segue uma estratégia formalmente análoga, mas em um domínio inteiramente diferente: a estrutura aparente (o transcript holomorfo) mascara — não, mais que isso, categorialmente exclui — a estrutura analítica privada (a completação modular). McEliece esconde por desordem aparente o que está estruturalmente presente. O Θ-Crypt elimina por ausência ontológica o que parecia estar presente. Os dois movimentos se relacionam como o anonimato em uma multidão (McEliece) se relaciona com a ausência absoluta (mock-theta).

Parte II — A Primeira Geração de Diversificadores (1979–1989)

Leslie Lamport: o minimalista sistêmico

Em 1979, em uma nota técnica da SRI International, Leslie Lamport propôs o primeiro esquema completo de assinatura digital baseado exclusivamente em funções de uma via — sem qualquer estrutura algébrica adicional. A construção é de uma simplicidade desarmante: para assinar uma única vez uma mensagem de n bits, gera-se 2n valores aleatórios (x_0^i, x_1^i) para i de 1 a n, publica-se a chave pública $H(x_0^i)$, $H(x_1^i)$ para uma função de hash H, e a assinatura de uma mensagem $m = (b_1, \ldots, b_n)$ é simplesmente o vetor $(x_{b_1}^1, \ldots, x_{b_n}^n)$.

O esquema é eficaz, mas tem o problema óbvio de ser de uso único — cada par de chaves só pode assinar uma mensagem. Foi Merkle quem, articulando em 1979 a estrutura de árvore que leva seu nome, mostrou como combinar exponencialmente muitas chaves Lamport em uma única chave pública agregada, dando origem à família de assinaturas hash-based que culmina no SPHINCS+ (2017) e no SLH-DSA padronizado (2024).

Lamport é, intelectualmente, o pai do minimalismo criptográfico. Sua tese implícita é: não confie em nada que você não absolutamente precise confiar. Não confie em fatoração, não confie em logaritmo discreto, não confie em redes, não confie em códigos. Confie apenas no que precisa minimamente existir para que haja qualquer criptografia: que existam funções unidirecionais. Tudo o mais é supérfluo.

A relação do programa mock-theta com Lamport é dialética. Em um sentido, o Θ-Crypt é o oposto de Lamport — é máximo, não mínimo; é estruturalmente ricamente determinado, não estruturalmente anêmico. Em outro sentido, é a sua continuação rigorosa: Lamport identificou que a segurança deve descansar sobre a menor base estrutural possível; o Θ-Crypt identifica que a segurança pode descansar sobre uma base estrutural impossível de capturar — não porque ela é simples, mas porque ela é, por construção, parcialmente fora do horizonte de identificabilidade do transcript público. Ambos os programas se afastam da confiança em problemas NP-difíceis dentro do paradigma de inversão. Lamport o faz por austeridade; mock-theta o faz por abundância modular.

Neal Koblitz e Victor Miller: a beleza geométrica

Em 1985, Neal Koblitz (na Universidade de Washington) e independentemente Victor Miller (na IBM Yorktown) propuseram substituir o grupo multiplicativo $(\mathbb{Z}/p\mathbb{Z})\times$ pelo grupo de pontos racionais de uma curva elíptica sobre um corpo finito, $E(\mathbb{F}_p)$. A motivação era principalmente eficiente: o problema do logaritmo discreto sobre $E(\mathbb{F}_p)$ resistia aos algoritmos sub-exponenciais (Index Calculus) que vinham erodindo a segurança do DH clássico, permitindo chaves muito menores para o mesmo nível de segurança.

Antes que ECC tornasse-se padrão industrial, contudo, é preciso registrar que as curvas elípticas já haviam desempenhado papel relevante na criptanálise — especificamente, no algoritmo de fatoração por curvas elípticas de Hendrik Lenstra (ECM), publicado em 1987 nos Annals of Mathematics. O método de Lenstra mostrou que objetos geométricos podiam alterar a paisagem computacional de problemas aritméticos clássicos: a curva não era apenas um desenho, era uma estrutura de grupo com propriedades aritméticas que podiam ser

exploradas algoritmicamente para acelerar a fatoração de inteiros com fatores primos de tamanho médio. Esse uso adversarial das curvas elípticas — primeiro como ferramenta de ataque, depois como fundamento de defesa — é tipicamente o padrão de maturação criptográfica: objetos matemáticos profundos primeiro testam os pressupostos existentes, e só depois são incorporados como novos fundamentos.

A elegância matemática da proposta Koblitz-Miller é profunda. As curvas elípticas são objetos riemann-roch que conectam geometria algébrica, formas modulares (via a conjectura de Taniyama-Shimura-Weil que Wiles provaria em 1995), análise p-ádica, e teoria de Galois. Quando Koblitz e Miller propuseram o ECC, estavam — sem necessariamente saberem disso na época — abrindo a porta para que toda a machinery da geometria aritmética moderna fosse posta a serviço da criptografia.

O ECC tornou-se, ao longo dos anos 1990 e 2000, o padrão de fato para criptografia móvel, IoT e comunicações de baixa largura de banda. Hoje em dia, virtualmente todo handshake TLS usa Curve25519 ou secp256r1 — descendentes diretos da proposta Koblitz-Miller.

Mas o ECC, exatamente como o DH clássico, satisfaz o ADU. O ponto público Q = dP determina unicamente o escalar privado d. E exatamente por isso, Shor o derrota. A redução do logaritmo discreto sobre E(𝔽_p) ao Hidden Subgroup Problem em ℤ/nℤ é direta — qualquer grupo cíclico finito é abeliano, e qualquer grupo abeliano finito é o playground natural da QFT.

A relação do programa mock-theta com Koblitz-Miller é instrutiva: o ECC mostrou que substituir a estrutura algébrica preservando o paradigma pode trazer ganhos de eficiência impressionantes — mas não escapa à fragilidade ontológica subjacente. A lição mais profunda do ECC, em retrospecto, é que a riqueza geométrica não basta; é preciso que a riqueza geométrica seja acompanhada por uma propriedade estrutural que escape ao paradigma de inversão. O ECC é beleza algébrica capturada no paradigma errado.

Kevin McCurley, Johannes Buchmann e Hugh Williams: o quase-salto

Já tratamos de McCurley na seção 3.2.5 do white paper. Aqui apenas reposicionamos sua contribuição no quadro genealógico.

McCurley, junto com a dupla Buchmann–Williams, foi o primeiro a propor um sistema criptográfico baseado em uma estrutura aritmética cuja própria ordem do grupo é estruturalmente difícil de calcular. O class number h(−d) não é apenas o tamanho do grupo de classes; é também o valor especial L(1, χ_d) · √|d| / π de uma L-função de Dirichlet — um objeto que carrega em si toda a profundidade da teoria analítica dos números.

A escolha de McCurley antecipa, com três décadas de antecedência, uma tese filosófica que só seria plenamente articulada no programa Θ-Crypt: os melhores fundamentos criptográficos são objetos matemáticos canônicos cuja dureza emerge naturalmente, não objetos artificiais cuja dureza é engenheirada. Class groups, formas modulares, curvas elípticas com multiplicação complexa, L-funções automorfas — toda essa família vive em uma única catedral matemática (o Langlands program), e o ataque a qualquer um deles é simultaneamente um ataque a toda a catedral. Esta é a forma mais robusta de hardness que se conhece — hardness por consenso da mais alta matemática.

McCurley, no entanto, manteve o ADU. Seu transcript público α = g^x ainda determina x unicamente. Foi a sua estrutura algébrica que diversificou, não o regime ontológico. A história fez ver: quando o moderno index calculus sobre grupos de classes amadureceu nos anos 2000, ficou claro que o sistema McCurley-Buchmann-Williams tinha o mesmo destino que o ECC sobre Shor.

E é aqui que a linha histórica se bifurca de forma elegante. Os descendentes diretos do programa McCurley são as isogenias — CSIDH, SCALLOP, SQIsign — que continuam apostando na riqueza aritmética dos grupos de classes e curvas com CM. Os descendentes diretos do programa Ramanujan, mediados por Zwegers e Zagier, são as mock theta functions — onde a mesma matemática de pontos CM e singular moduli reaparece, agora do lado analítico-modular em vez do algébrico-aritmético, e onde a propriedade-chave não é a opacidade computacional mas a ausência categorial da informação que selecionaria o segredo.

Hafner-McCurley-Buchmann: a computação efetiva como exigência criptográfica

A contribuição de McCurley não pode ser plenamente apreciada sem referência ao trabalho técnico que a acompanhou e que a tornou criptograficamente viável. A passagem de uma estrutura aritmética para uma plataforma criptográfica exige uma disciplina que pode ser chamada de computação efetiva. Não basta saber que um grupo existe, que uma classe está bem definida ou que um teorema assintótico descreve seu tamanho médio. É preciso calcular, amostrar, reduzir, representar e comparar. A teoria algébrica dos números computacional transformou objetos antes contemplativos em objetos manipuláveis por máquinas — e nesse ambiente, os trabalhos de James Hafner e Kevin McCurley sobre algoritmos probabilísticos subexponenciais para o cálculo de grupos de classes, e os de Johannes Buchmann sobre reduções e equivalências, foram decisivos.

Buchmann merece destaque particular porque sua obra atravessa tanto a teoria de grupos de classes quanto a formação posterior da criptografia pós-quântica como campo organizado. Ele ajudou a consolidar a ideia de que a segurança futura deveria considerar uma pluralidade de pressupostos matemáticos. Sua associação editorial e científica com o volume canônico Post-Quantum Cryptography (Bernstein-Buchmann-Dahmen, Springer 2009) expressa essa transição. A comunidade deixou de tratar alternativas como exotismos dispersos e passou a organizar famílias: lattice-based, code-based, hash-based, multivariate, isogeny-based. Essa classificação parece natural hoje, mas é resultado de décadas de maturação institucional — e Buchmann é uma das figuras-chave nessa institucionalização.

A computação de números de classe também é relevante por outra razão filosoficamente decisiva. Ela exemplifica o modo como a teoria analítica dos números entra na criptografia. Estimativas de distribuição, funções L, hipóteses generalizadas de Riemann, constantes efetivas e fenômenos assintóticos deixam de ser apenas instrumentos de prova e tornam-se parâmetros de segurança. A criptografia moderna herdou da teoria dos números não apenas objetos, mas também uma atitude: perguntar como uma estrutura se distribui, que exceções existem, que algoritmos exploram regularidades, e que hipóteses são necessárias para garantir tempo de execução. Essa atitude é diretamente aplicável a qualquer programa baseado em mock theta functions. Antes

de falar em chaves, será preciso falar em distribuição de coeficientes, crescimento, dependência entre termos, órbitas modulares e possíveis algoritmos de reconstrução.

A história de McCurley-Hafner-Buchmann revela que a criptografia pós-quântica não é somente a busca por sistemas que Shor não quebre. É a busca por uma engenharia de pressupostos. Cada pressuposto deve ser explícito, comparável e atacável. A maturidade criptográfica surge quando uma comunidade consegue dizer não apenas "não conhecemos ataque", mas "sabemos quais ataques procurar, quais reduções sustentam a dificuldade, quais parâmetros evitam degenerações e quais hipóteses matemáticas estão sendo assumidas". Esse é o patamar que qualquer sistema novo, inclusive um Mock Theta Function Cryptographic System, deve ambicionar — e qualquer pretensão menor a esse padrão deve ser tratada como retórica imatura, não como ciência criptográfica.

Parte III — O Cataclismo Quântico (1994–1996)

Peter Shor: a revelação ontológica

Em abril de 1994, em um seminário na 35th Annual Symposium on Foundations of Computer Science em Santa Fe, Peter Shor, pesquisador da Bell Labs, apresentou Algorithms for Quantum Computation: Discrete Logarithms and Factoring. O paper completo, publicado depois no SIAM Journal on Computing, demonstrou que um computador quântico universal — ainda hipotético na época — pode fatorar inteiros e calcular logaritmos discretos em tempo polinomial.

A maneira correta de entender Shor é a seguinte. Ele não inventou um algoritmo isolado; ele unificou uma classe inteira de problemas sob um arcabouço único — o Hidden Subgroup Problem (HSP). Dado um grupo G e uma função f: G → S tal que f seja constante em cosets de um subgrupo desconhecido H ≤ G, o HSP consiste em determinar H. Shor mostrou que, quando G é abeliano, este problema é solúvel em tempo quântico polinomial via Quantum Fourier Transform sobre G.

A consequência é devastadora — e a palavra é mal escolhida apenas se subestima a sua amplitude. Toda a criptografia clássica baseada em grupos abelianos finitos cai. Fatoração? É HSP em $(\mathbb{Z}/N\mathbb{Z})^\times$. Logaritmo discreto em $\mathbb{F}_p^\times$? HSP em $\mathbb{Z}/(p-1)\mathbb{Z}$. ECDLP? HSP em $\mathbb{Z}/n\mathbb{Z}$ onde n é a ordem do ponto base. McCurley-Buchmann-Williams? HSP em $\mathrm{Cl}(\mathcal{O}_K)$. Tudo.

O ponto filosoficamente mais importante de Shor, e que o discurso usual da criptografia pós-quântica frequentemente perde, é este: Shor não está descobrindo que essas estruturas são acidentalmente vulneráveis. Ele está demonstrando que elas são estruturalmente vulneráveis. A vulnerabilidade está embutida na definição mesma de "grupo abeliano com inversão de período oculto". Não há um patch que possa ser aplicado. Não há uma escolha mais inteligente de parâmetros que possa salvar o esquema. A vulnerabilidade é a estrutura.

E é exatamente esta percepção que o programa mock-theta toma como ponto de partida. O Θ-Crypt nasce não da pergunta "como construir um problema de inversão difícil mesmo para Shor?" — essa pergunta é a do programa NIST e produz Kyber, Dilithium, etc. O Θ-Crypt nasce da pergunta filosoficamente anterior: e se a relação entre público e privado não fosse uma relação de inversão? E se a estrutura matemática subjacente permitisse construir esquemas em que o privado não está categorialmente presente no público?

A resposta a essa pergunta é o que distingue o programa Θ-Crypt de tudo o que veio antes. E é por isso que Shor, mais do que ameaça, é fundador. Sem Shor, ninguém teria pensado em buscar a propriedade que Ramanujan, sem saber, havia preparado nas mock theta functions.

Lov Grover: a ameaça assintótica

Em 1996, Lov Grover, também na Bell Labs, demonstrou que um computador quântico pode realizar buscas em espaços não-estruturados com vantagem quadrática sobre algoritmos clássicos. O algoritmo de Grover oferece $O(\sqrt{N})$ chamadas a uma função oráculo para encontrar um elemento marcado em um espaço de N candidatos, contra $O(N)$ classicamente.

A implicação para a criptografia é mais sutil do que Shor. Grover não derruba nenhum esquema; ele apenas halva o expoente da segurança. Chaves AES de 128 bits passam a ter segurança efetiva de 64 bits frente a um adversário Grover, e por isso o padrão NIST passou a recomendar AES-256 para uso pós-quântico. Para criptografia simétrica e hashes, a resposta a Grover é simplesmente dobrar o tamanho das chaves e das saídas de hash.

Mas o programa mock-theta enfrenta Grover de uma forma específica e elegante que vale comentar. Como o Θ-Crypt opera em um espaço de completações modulares cuja largura de ambiguidade é, por construção, exponencialmente grande, o ganho quadrático de Grover ainda deixa um espaço de busca exponencialmente intratável. Mais que isso: a estrutura analítica do mock-theta permite uma construção que chamamos de Coherent Ambiguity Dispersion (CAD), em que a busca de Grover precisa, na verdade, ser dispersa por um conjunto de orientações inequivalentes do completion shadow — elevando o custo de O(√M) para O(M^{2/3}), uma resistência superior ao requisito NIST-V.

Grover, no espírito do programa mock-theta, é portanto não uma ameaça mas um teste de robustez: o sistema é projetado de tal modo que mesmo o tipo mais genérico de vantagem quântica — que não depende de nenhuma estrutura algébrica explorável — é atenuado por construção.

Parte IV — O Renascimento Reticular (1996–2009)

Miklós Ajtai: a redução worst-case to average-case

A família lattice-based tornou-se o eixo dominante da padronização pós-quântica contemporânea. Para entender essa dominância, é necessário voltar a um precursor cuja importância é frequentemente subestimada: o algoritmo LLL de Hendrik Lenstra, Arjen Lenstra e László Lovász, publicado em 1982 na Mathematische Annalen. O LLL mostrou que reticulados podiam ser reduzidos de forma eficiente em certo sentido aproximado — uma descoberta com consequências que se estenderam por toda a criptografia subsequente, tanto como ferramenta construtiva quanto como instrumento de ataque. Claus-Peter Schnorr, em 1987, aprofundou essa tradição com hierarquias de redução (BKZ) e técnicas práticas que influenciaram tanto criptanálise quanto construções, refinando o entendimento de quão próximos de vetores ótimos algoritmos polinomiais conseguem chegar.

Reticulados são objetos geométricos discretos em espaços de alta dimensão. Seus problemas clássicos — Shortest Vector Problem (SVP), Closest Vector Problem (CVP), e suas variantes aproximadas — combinam simplicidade de enunciado com dificuldade computacional aparente. O LLL e seus sucessores Schnorrianos definiram, durante a década de 1980, o regime de pensamento que tornaria reticulados criptograficamente viáveis: dimensão alta, ruído controlado, aproximação como métrica de dureza, redução de base como ferramenta universal. Sem essa preparação técnica acumulada, o salto de Ajtai-Regev na década seguinte não teria sido possível.

Em 1996, em um paper que mudou o campo, Miklós Ajtai (na IBM Almaden, curiosamente o mesmo laboratório de McCurley) provou um teorema que, à primeira vista, parecia técnico demais para ter consequências revolucionárias. Ajtai demonstrou que resolver o problema Short Integer Solution (SIS) em média implica resolver problemas de reticulado no pior caso — especificamente, encontrar vetores curtos em qualquer rede de uma classe específica.

Esta redução worst-case to average-case é, em retrospecto, o resultado mais importante da teoria de criptografia desde a função alçapão de Diffie-Hellman. Por quê? Porque resolve um problema epistemológico fundamental da criptografia: como garantir que uma instância aleatoriamente escolhida do problema é de fato difícil?

Em todas as criptografias anteriores — RSA, DH, ECC — a hipótese de dureza é estatística: acreditamos que números semiprimos aleatórios são difíceis de fatorar, mas não conseguimos provar a partir de hipóteses padrão da complexidade computacional. Pode existir uma classe especial de números aleatoriamente gerados que seja fácil de fatorar; só sabemos que essa classe, se existir, tem medida pequena. A redução de Ajtai elimina esse problema: a hipótese de dureza torna-se uma hipótese sobre o pior caso de uma classe natural de problemas geométricos — uma hipótese que é, por natureza, muito mais sólida.

A consequência foi a explosão da criptografia baseada em reticulados. Ajtai-Dwork em 1997 produziu o primeiro criptosistema reticular completo. Hoffstein-Pipher-Silverman, no mesmo ano, propuseram independentemente o NTRU, mais prático mas com fundamento heurístico mais frágil. Foi Oded Regev, em

2005, quem completou o programa de Ajtai propondo o problema Learning With Errors (LWE) e provando uma redução quântica de LWE para problemas reticulares no pior caso. A partir de Regev, a criptografia reticular tornou-se a candidata mais robusta para padronização pós-quântica.

O ML-KEM (Kyber) e o ML-DSA (Dilithium) padronizados pelo NIST em 2024 são descendentes diretos do programa Ajtai-Regev, refinados via Module-LWE para eficiência prática.

A relação do programa mock-theta com Ajtai-Regev é particularmente delicada e merece articulação cuidadosa. O programa reticular conquistou uma vitória ontológica importante: ele eliminou a redução estatística e fundamentou a dureza criptográfica em hipóteses geométricas sólidas. Mas, do ponto de vista do ADU, ele não representa uma mudança. A chave pública de Kyber é uma matriz A junto com um vetor b = As + e, e o vetor secreto s está determinado pelo par (A, b) — apenas sua extração é (presumivelmente) computacionalmente difícil. O ADU está intacto. A segurança é, exatamente como em RSA, uma segurança por inversão difícil.

E é exatamente aqui que a vulnerabilidade categorial dos reticulados se manifesta. Se um avanço algoritmico — clássico ou quântico — for descoberto que resolve LWE eficientemente, todo o catálogo NIST cai simultaneamente. Kyber, Dilithium, Falcon — todos são variações estruturadas do mesmo problema fundamental. O programa mock-theta argumenta, com base na história de SIKE, que esta concentração ontológica é precisamente o risco que a criptografia pós-quântica precisa diversificar — não com mais um sabor de reticulado, mas com uma família matemática genuinamente diferente.

Hoffstein, Pipher e Silverman: a praticidade do NTRU

Em 1996, três matemáticos da Brown University — Jeffrey Hoffstein, Jill Pipher e Joseph Silverman — propuseram independentemente um sistema reticular muito mais prático que Ajtai-Dwork, embora com fundamentos teóricos inicialmente menos rigorosos: o NTRU. A construção opera em um anel quociente $\mathbb{Z}[x]/(x^n - 1)$ ou $\mathbb{Z}[x]/(x^n + 1)$, explora a estrutura cíclica para eficiência, e tem chaves e cifrações muito menores do que Ajtai-Dwork.

NTRU é o ancestral direto do FALCON (FN-DSA), padronizado pelo NIST em 2024 como FIPS 206. Sua história é didática para o programa Θ-Crypt: NTRU mostra que a praticidade pode emergir de uma rica estrutura algébrica subjacente, sem comprometer a segurança. O sistema usa elementos do anel ciclotômico para reduzir tamanhos de chave em uma ordem de magnitude relativamente a reticulados não-estruturados.

A relação do mock-theta com NTRU é a do programa que aprende a lição da estrutura algébrica fina mas a aplica em outro plano. Onde NTRU usa a estrutura ciclotômica de $\mathbb{Z}[x]/(x^n + 1)$, o Θ-Crypt usa a estrutura modular de espaços de formas de Maass harmônicas associadas a grupos congruentes $\Gamma_0(N)$. Em ambos os casos, a riqueza algébrica subjacente é o que permite construções eficientes; em ambos os casos, há um risco residual de que essa riqueza seja explorável por um adversário suficientemente sofisticado.

A diferença crítica é que NTRU continua dentro do ADU: o par (h, n) determina o privado (f, g). O Θ-Crypt opera em um espaço onde a relação entre os dados públicos e o segredo é mediada por uma propriedade

cohomológica não-trivial (o shadow $\mathfrak{g}^-$ vivendo na completação harmônica) que nunca aparece no transcript público — e é essa propriedade que rompe categorialmente o ADU.

Oded Regev: o LWE e a fundação moderna

Em 2005, Oded Regev (então em Tel Aviv) propôs o problema Learning With Errors (LWE) e provou que ele é tão difícil quanto problemas reticulares no pior caso — sob a hipótese de que algoritmos quânticos não resolvem certos problemas reticulares eficientemente. O LWE substituiu rapidamente a formulação original de Ajtai como o problema-fundamento da criptografia reticular moderna.

A elegância do LWE está em sua simplicidade: dado $(A, b = As + e)$ com e um vetor de ruído gaussiano, encontre s. A versão decisional — distinguir entre amostras LWE legítimas e amostras uniformes aleatórias — é particularmente útil para construções criptográficas, e foi o que Regev usou para construir o primeiro KEM reticular eficiente.

O Kyber (ML-KEM) é, essencialmente, LWE estruturado via módulos sobre anéis ciclotômicos para eficiência prática. O Dilithium (ML-DSA) é a versão de assinatura. Toda a infraestrutura de chave pública pós-quântica que o mundo está adotando entre 2024 e 2030 descansa, em última análise, sobre a hipótese de Regev — que problemas reticulares no pior caso resistem a algoritmos quânticos.

A relação do programa mock-theta com Regev é a do contraponto intelectualmente honesto. Regev produziu, sem sombra de dúvida, o maior avanço estrutural na criptografia desde Diffie-Hellman. Sua redução worst-case to average-case via mecanismos quânticos é uma das peças mais elegantes da teoria de complexidade. O Θ-Crypt não compete com o LWE; complementa-o. O argumento é o que articulamos antes: mesmo Regev satisfaz o ADU. Se o LWE cair — e há sinais cada vez mais audíveis de que ataques híbridos quânticos sobre estruturas reticulares específicas podem oferecer melhorias subexponenciais — toda a infraestrutura mundial cai junto. Hedge ontológico significa, no contexto pós-quântico de 2026, ter uma família matemática genuinamente diferente disponível como sistema de backup. Essa é a função do mock-theta.

Parte V — A Cristalização (2009–2024)

Daniel J. Bernstein: o sintetizador

Se há uma figura que personifica a maturidade da criptografia pós-quântica, é Daniel J. Bernstein — matemático, programador, ativista, e produtor de literalmente metade das ferramentas práticas que o campo usa hoje. SPHINCS, NTRU Prime, McBits, Classic McEliece, Ed25519, X25519, Salsa20, ChaCha20 — a marca de Bernstein está em toda parte.

A contribuição de Bernstein para o que chamamos hoje de criptografia pós-quântica não é uma construção isolada, é uma postura intelectual. Em 2009, junto com Johannes Buchmann (o mesmo do esquema BW de class groups) e Erik Dahmen, Bernstein editou o livro Post-Quantum Cryptography — o primeiro tratamento sistemático do campo como disciplina, que efetivamente batiza a área. O livro reúne contribuições sobre lattices, código, hash, multivariáveis e isogenias, articulando pela primeira vez o que viria a ser o framework de diversificação de famílias que o NIST adotaria sete anos depois.

A relação do programa mock-theta com Bernstein é a do herdeiro que estende a postura sintetizadora a uma nova família. Bernstein argumentou desde 2009 que a criptografia pós-quântica não deve apostar tudo em uma família — deve manter múltiplas famílias maduras, prontas para substituição em caso de quebra inesperada. O Θ-Crypt se posiciona como a sexta família — distinta de lattices, codes, hashes, multivariate e isogenies, com fundamento em formas modulares de Maass e mock theta functions de Ramanujan. Em 2026, esta é a única família genuinamente nova proposta nas últimas duas décadas.

O processo NIST: padronização e crítica

Entre 2016 e 2024, o NIST conduziu o processo de padronização de criptografia pós-quântica mais rigoroso da história. Sessenta e nove submissões iniciais foram reduzidas, em quatro rodadas de escrutínio público, a quatro padrões oficiais: ML-KEM (Kyber, FIPS 203), ML-DSA (Dilithium, FIPS 204), SLH-DSA (SPHINCS+, FIPS 205) e FN-DSA (FALCON, FIPS 206). Em 2025, HQC (code-based) foi adicionado como alternativa a Kyber.

O processo NIST é, ao mesmo tempo, uma conquista monumental e um diagnóstico parcial. Conquista, porque produziu pela primeira vez na história padrões criptográficos com escrutínio público massivo, implementações de referência auditáveis, e adoção governamental coordenada. Diagnóstico parcial, porque três dos quatro padrões originais (Kyber, Dilithium, Falcon) são todos baseados em problemas reticulares — uma concentração que o próprio NIST reconhece como risco e tenta mitigar com a recomendação de implementações híbridas.

A relação do programa mock-theta com o processo NIST é de complementaridade explícita. O Θ-Crypt não pretende substituir o NIST PQC — pretende oferecer uma camada adicional de defesa em profundidade, especificamente projetada para dados de altíssima sensibilidade e longo período de proteção. Hybrid mode

sobre Kyber + Θ-KEM é a recomendação técnica natural para aplicações de defesa, infraestrutura crítica e proteção de dados de inteligência.

A transição como tarefa de engenharia histórica

Há uma dimensão da era pós-quântica que merece nomeação explícita porque, embora seja a mais imediata e operacionalmente relevante de todas, costuma ser ofuscada pelo brilho dos resultados teóricos. A transição pós-quântica é, ao mesmo tempo, uma tarefa matemática e uma tarefa de engenharia histórica de escala civilizacional. Protocolos precisam ser atualizados, certificados precisam mudar, bibliotecas precisam implementar novas primitivas, hardware precisa suportar chaves e assinaturas de tamanhos significativamente diferentes, e organizações precisam lidar com a ameaça denominada harvest now, decrypt later — segundo a qual dados capturados hoje, no estado atual da criptografia, podem ser descriptografados retrospectivamente assim que computadores quânticos suficientemente grandes estiverem disponíveis, o que torna a migração não apenas uma questão de proteção futura mas de proteção retroativa.

A criptografia deixa então de ser apenas problema de matemáticos e torna-se problema de administração de infraestrutura global. Calendários de migração definidos por NSA (CNSA 2.0, 2030), BSI alemão, ANSSI francês, NCSC britânico e ENISA europeia estabelecem prazos concretos para a substituição de RSA e ECC em sistemas de alto valor estratégico. O Brasil, neste contexto, encontra-se em posição estratégica peculiar: ainda não há cronograma nacional formal de transição, e a infraestrutura crítica brasileira — telecomunicações, sistemas financeiros, defesa nacional, governo digital — opera majoritariamente sobre primitivas criptográficas vulneráveis ao paradigma de Shor. O programa Θ-Crypt insere-se nesse vácuo institucional como proposta de capacidade soberana, ao mesmo tempo defensiva (proteção de dados) e científica (formação de quadro técnico nacional em criptografia avançada).

Nesse ambiente operacional, qualquer proposta não canônica como o Mock Theta Function Cryptographic System deve compreender com clareza sua posição estratégica. Ela não compete imediatamente com ML-KEM como padrão operacional de mercado. Ela opera em outra camada — a camada de pesquisa fundamental, onde novas famílias de pressupostos podem ser formuladas e preparadas para o caso de quebra inesperada das famílias dominantes. A história mostra que essa camada é indispensável. Sem ela, a padronização futura se torna repetição de uma monocultura. Com ela, a comunidade preserva opções para crises ainda não previstas.

Parte VI — Os Desvios: Isogenias e o Aviso de SIKE

Há uma linha lateral importante a registrar antes de chegar ao programa mock-theta propriamente dito, porque ela funciona como aviso histórico crítico. Em 1997, Jean-Marc Couveignes escreveu um manuscrito não-publicado propondo criptografia baseada em isogenias entre curvas elípticas. A ideia foi independentemente redescoberta por Alexander Rostovtsev e Anton Stolbunov em 2006. Em 2011, Luca De Feo, David Jao e Jérôme Plût propuseram o SIDH (Supersingular Isogeny Diffie-Hellman), que tornou-se rapidamente o candidato pós-quântico mais elegante: chaves pequenas, fundamento matemático profundo (isogenias entre curvas elípticas supersingulares sobre $\mathbb{F}_{p^2}$), e aparente resistência tanto a Shor quanto a Grover.

O SIDH evoluiu para o SIKE, que foi finalista NIST por seis anos.

E então, em julho de 2022, Wouter Castryck e Thomas Decru publicaram um ataque clássico — não quântico — em tempo polinomial que quebra completamente o SIDH/SIKE. O NIST retirou o SIKE em agosto. Seis anos de escrutínio público de elite, dezenas de papers, várias implementações industriais — tudo dissolvido em um único paper de 39 páginas.

A lição de SIKE é a mais sóbria que a história recente da criptografia oferece, e ela alimenta diretamente a justificativa estratégica do programa Θ-Crypt. Esquemas baseados em estruturas algebraicamente ricas — especialmente aquelas em que a estrutura é exposta no transcript público — são vulneráveis a ataques clássicos inesperados que exploram propriedades estruturais que ninguém pensou em explorar antes. A monocultura de qualquer tipo, mesmo a monocultura de "famílias matematicamente sofisticadas que parecem seguras", é um risco.

A relação do programa mock-theta com o desastre SIKE é, então, dupla. Por um lado, SIKE valida a tese central do mock-theta: a diversificação ontológica é uma necessidade estratégica, não um luxo acadêmico. Por outro, a metodologia mock-theta é especificamente projetada para não expor propriedades estruturais exploráveis: o transcript holomorfo T é, por construção, categorialmente insuficiente para reconstruir a completação G. Não há propriedade estrutural escondida a descobrir — porque a estrutura privada simplesmente não está no transcript público.

Há uma terceira leitura de SIKE, contudo, que merece ser articulada com a serenidade que a historiografia científica exige. SIKE não deve ser lembrado apenas como fracasso. Deve ser lembrado também como vitória do método científico em criptografia. Um candidato promissor foi submetido a escrutínio público durante seis anos, um ataque brilhante foi encontrado por dois pesquisadores belgas trabalhando em geometria aritmética de curvas com gênero superior, e a comunidade ajustou suas expectativas em questão de semanas. Essa é a regra do campo. A legitimidade de uma nova direção criptográfica não vem de sobreviver sem ser atacada — vem de sobreviver depois de ser atacada por especialistas independentes durante tempo suficiente. SIKE cumpriu o lado científico do contrato: foi proposto com rigor, escrutinado com rigor, e quando fragilizado, retirado com rigor. O fracasso técnico foi acompanhado de sucesso metodológico. Essa lição é essencial para qualquer programa novo, inclusive o Θ-Crypt: pertencer seriamente à genealogia pós-quântica significa

construir para esse tipo de exposição, não tentar evitá-la. Um sistema que evita ataques ganha apenas obscuridade; um sistema que os recebe e sobrevive ganha credibilidade científica.

Há também uma lição metodológica adicional que SIKE oferece e que o programa mock-theta deve assimilar explicitamente: profundidade matemática não equivale automaticamente a segurança. Um objeto pode ser sofisticado, belo e ainda assim possuir uma estrutura explorável de forma inesperada. Essa lição é particularmente relevante para mock theta functions. O fato de uma família matemática ser profunda, historicamente misteriosa ou ligada a Ramanujan não a torna criptograficamente segura. Pelo contrário, sua profundidade aumenta tanto o potencial quanto o risco. Estrutura rica pode oferecer hard problems; pode também oferecer atalhos. Fenômenos modulares podem produzir pseudorandomness aparente; podem também produzir regularidades exploráveis. O programa só será sério se aceitar essa ambivalência desde o início — e organizar sua própria criptanálise adversarial como parte constitutiva da pesquisa, não como etapa posterior.

Parte VII — Ramanujan, Zwegers, Zagier: A Linhagem Mock-Theta

Srinivasa Ramanujan: a carta de janeiro de 1920

I discovered very interesting functions recently which I call "Mock" θ-functions…
— S. Ramanujan, carta a G. H. Hardy, 12 de janeiro de 1920

Em 12 de janeiro de 1920, três meses antes de sua morte em Kumbakonam, Srinivasa Ramanujan escreveu sua última carta a G. H. Hardy. Tinha 32 anos, estava tuberculoso, e dispunha de algumas semanas de lucidez restantes. A carta, hoje conhecida como a deathbed letter, contém uma das contribuições matemáticas mais misteriosas do século XX: a introdução de dezessete mock theta functions.

Ramanujan as apresentou sem definição rigorosa. Disse apenas que eram funções definidas por séries q-expansíveis que se comportavam, ao se aproximarem de pontos racionais do círculo unitário, quase como theta functions clássicas — exibindo padrões de explosão controlados por outras funções modulares — mas que não eram, elas próprias, modulares. Listou exemplos do tipo:

$$f(q) = \Sigma\, q\text{^}\{n^2\} / [(1+q)^2(1+q^2)^2 \cdots (1+q\text{^}n)^2]$$

e variantes em três ordens de "profundidade" (third order, fifth order, seventh order), totalizando dezessete funções específicas.

Hardy, recebendo a carta em Cambridge, ficou perplexo. Ramanujan não explicava o que tornava essas funções "mock"; apenas afirmava que se comportavam de uma maneira específica perto da fronteira do disco. Por oitenta anos, matemáticos trabalharam tentando entender o que Ramanujan havia visto — sem conseguir produzir uma definição satisfatória do que era uma mock theta function. Watson, em seu paper de 1936 The final problem: an account of the mock theta functions no Journal of the London Mathematical Society, Selberg, George Andrews em sua redescoberta do Lost Notebook em 1976, Hickerson com sua prova das identidades de quinta ordem em 1988 — todos contribuíram com pedaços do quebra-cabeças. Mas o objeto permanecia ontologicamente esquivo, ocupando uma posição intermediária e desconfortável entre as formas modulares clássicas e meras q-séries arbitrárias.

A modernidade das mock theta functions está precisamente em sua posição intermediária — em sua simultânea rigidez e anomalia. Elas não são modular forms clássicas, mas também não são q-séries arbitrárias. Possuem coeficientes, transformações, assintóticas, sombras e completions. Essa mistura, durante o século XX, gerou ligações inesperadas com objetos aparentemente distantes: partições com restrições combinatórias, formas de Maass não-holomorfas, Borcherds products em teoria de cordas, valores centrais de L-functions, invariantes de variedades de Calabi-Yau, e até mesmo entropias de buracos negros em física matemática via o trabalho de Atish Dabholkar, Sameer Murthy e Don Zagier. Para a matemática pura, mock theta functions revelaram-se um nó central de conexões transversais. Para a criptografia — e esta é a pergunta que o programa Θ-Crypt formula —, a pergunta ainda é embrionária: há nesse território algum problema computacional natural, parametrizável e resistente a ataques clássicos e quânticos conhecidos? A resposta a essa pergunta é o programa de pesquisa que articularemos formalmente na próxima parte deste ensaio.

Sander Zwegers: a tese de 2002

Em 2002, em Utrecht, sob a orientação de Don Zagier, o jovem holandês Sander Zwegers defendeu uma tese de doutorado que finalmente revelou o que Ramanujan havia visto. O resultado central de Zwegers é o seguinte: uma mock theta function não é uma forma modular, mas pode ser completada a uma forma de Maass harmônica adicionando um termo não-holomorfo específico.

Mais precisamente: seja f(τ) uma mock theta function. Existe uma única função g(τ) — chamada de shadow de f — tal que a combinação

$$\hat{f}(\tau) = f(\tau) + g^*(\tau)$$

(onde g* é uma integral específica relacionada a g) é uma forma de Maass harmônica genuína, transformando-se modularmente sob Γ_0(N) para algum nível N. A função f̂ é modular, mas é não-holomorfa. A parte holomorfa f é o que Ramanujan observava; a parte não-holomorfa g* é o que estava estruturalmente ausente da observação.

Zwegers, em outras palavras, mostrou que cada mock theta function é a parte holomorfa de um objeto modular completo de Maass — mas que essa parte holomorfa não determina o todo. Há uma componente analítica (a shadow) que vive em um setor anti-holomorfo e que, por sua natureza, nunca aparece nos coeficientes de Fourier holomorfos.

Esta é, exatamente, a propriedade que o programa Θ-Crypt operacionaliza criptograficamente. O transcript público T é precisamente os coeficientes holomorfos. O segredo G é precisamente a shadow. A relação entre eles não é uma relação de inversão difícil — é uma relação de complementaridade categorial.

Don Zagier, Kathrin Bringmann, Ken Ono: o programa moderno

Após a tese de Zwegers, o campo de mock modular forms explodiu. Don Zagier, em 2007, conectou as mock theta functions a singular moduli — os valores da função j em pontos CM. Kathrin Bringmann, Amanda Folsom e Ken Ono produziram, ao longo dos anos 2010, uma teoria sistemática conectando mock theta functions a black holes em teoria de cordas, a partitions, a representations de Kac-Moody, e — crucialmente — a L-functions de objetos automorfos não-clássicos.

Esta moderna teoria das mock modular forms é, hoje, um campo florescente da teoria dos números, com aplicações em física teórica, combinatória, e — agora — em criptografia.

A síntese matemática que o programa Θ-Crypt realiza é a seguinte: as mock theta functions vivem em um espaço cohomológico não-trivial $H^1(\Gamma_0(N), V)$, onde V é uma representação de Γ_0(N) adequada. A classe cohomológica de uma mock theta function é determinada parcialmente pelos seus coeficientes holomorfos (o transcript) e parcialmente pela sua shadow (o segredo). A operação criptográfica é: o emissor escolhe uma classe cohomológica; publica os coeficientes holomorfos; mantém a shadow privada. A verificação ocorre por meio de operadores de Hecke aplicados à completação, que permitem ao destinatário (possuindo a shadow) recuperar a mensagem, mas que não permitem a um adversário, possuindo apenas o transcript holomorfo, fazer o mesmo.

Esta é, em essência, uma criptografia em que o segredo não está oculto — está categorialmente ausente do público. E é nessa diferença que reside toda a robustez frente a Shor: não há HSP para Shor resolver, porque não há grupo a inspecionar; a estrutura não é grupo-teórica, é modular-analítica.

Parte VIII — Síntese: Como Cada Pai Apontou Para a Solução

Voltemos ao fio condutor que prometemos no início. Cada pai da criptografia pós-quântica, na sua decisão fundadora, apontou para uma propriedade estrutural que ele próprio não soube nomear plenamente — e que o programa mock-theta realiza.

Merkle apontou para a *eliminação de estrutura algébrica supérflua*. Mostrou que a segurança pode emergir de funções de uma via puras, sem nenhum grupo, anel ou corpo. O Θ-Crypt herda essa lição: também não confia em estrutura algébrica clássica, mas a substitui não por hashes (como Merkle) mas por estrutura modular-analítica — uma forma de *opacidade rica* que é o oposto técnico, mas o irmão filosófico, da *opacidade pobre* do hash.

Diffie-Hellman apontaram para a *contingência da escolha do grupo*. Sabiam, em 1976, que o $(\mathbb{Z}/p\mathbb{Z})^\times$ era escolha arbitrária. O Θ-Crypt completa o programa de re-escolha: substitui o grupo por uma estrutura modular completamente fora do paradigma grupo-teórico.

Rivest-Shamir-Adleman apontaram para o *risco da monocultura ontológica*. Não como tese explícita, mas como consequência observada. O Θ-Crypt é a primeira família matemática que se propõe explicitamente como hedge contra essa monocultura.

McEliece apontou para o *valor de problemas estruturalmente diversos do mainstream*. Em 1978, era marginal; em 2024, é candidato oficial NIST. O Θ-Crypt segue essa estratégia de marginalidade ontológica deliberada como hedge histórico.

Lamport apontou para a *separação radical entre o que precisa estar oculto e o que pode ser exposto*. O Θ-Crypt opera com a separação categorial mais radical possível: o que precisa estar oculto (a shadow) está categorialmente ausente do que é exposto (o transcript holomorfo).

Koblitz-Miller apontaram para a *riqueza geométrica como fonte de robustez*. O Θ-Crypt herda a riqueza, transferindo-a do plano algébrico-aritmético (curvas elípticas) para o plano modular-analítico (formas de Maass harmônicas).

McCurley apontou para a *diversificação dos fundamentos como necessidade estratégica*. Foi quase o último passo. O programa Θ-Crypt o completa, diversificando não a estrutura algébrica mas o regime ontológico.

Shor apontou para a *fragilidade categorial do ADU*. Sua demonstração de que QFT resolve HSP abeliano é simultaneamente a maior ameaça e a maior lição: o ADU é a fragilidade, não a fatoração. O Θ-Crypt elimina o ADU.

Grover apontou para a *necessidade de espaços de busca exponencialmente grandes mesmo na ausência de estrutura explorável*. O Θ-Crypt, pela largura de ambiguidade exponencial da shadow, satisfaz essa necessidade por construção.

Ajtai-Regev apontaram para o *valor de hipóteses de dureza worst-case-rigorosas*. O Θ-Crypt, fundamentando-se em propriedades de não-identificabilidade ligadas à teoria de Hecke e à teoria de representação de GL_2, oferece um análogo: a dureza não é estatística, é estrutural-cohomológica.

Bernstein apontou para a *necessidade de famílias plurais de fundamentos*. O Θ-Crypt é a sexta família proposta — e, em 2026, a única genuinamente nova.

Castryck-Decru, com a quebra de SIKE, apontaram para o *risco de propriedades estruturais escondidas em transcripts públicos*. O Θ-Crypt, por construção, não tem propriedades estruturais escondidas — a estrutura privada não está no transcript.

Ramanujan-Zwegers-Zagier apontaram para a *existência de objetos matemáticos canônicos com complementaridade ontológica entre componentes públicas e privadas*. O programa Θ-Crypt é a primeira operacionalização criptográfica explícita dessa descoberta.

A imagem completa é a de uma sucessão de pais que, cada um a seu modo, antecipou uma faceta da solução, sem nunca conseguir reunir todas as facetas em um objeto único. O Θ-Crypt é o objeto único — não porque seja superior aos seus antecessores, mas porque cumpre uma promessa que cinquenta anos de criptografia foram fazendo em segmentos.

Parte IX — Esboço de uma Agenda Formal para o Programa Mock-Theta

Uma genealogia seria incompleta sem o esboço das etapas formais que separam um programa de pesquisa de uma família criptográfica madura. As seções precedentes posicionaram o programa Mock Theta Function Cryptographic System dentro de uma linhagem intelectual legítima; esta seção articula, com sobriedade técnica, as etapas que esse programa deve cumprir para passar do estágio de hipótese para o estágio de sistema validado. A apresentação segue dois eixos complementares: cinco eixos temáticos de investigação que delimitam o conteúdo matemático da pesquisa, e sete etapas metodológicas que delimitam seu processo institucional.

Cinco eixos temáticos de investigação

O primeiro eixo é o problema de inversão de coeficientes. Dada uma família $F_\lambda(q) = \Sigma\, a_n(\lambda)\, q^n$, parametrizada por λ em um espaço discreto ou aritmético, pergunta-se se observações parciais de $a_n(\lambda)$, possivelmente misturadas com ruído, truncamento, mascaramento ou transformações, permitem recuperar λ. A dificuldade desse problema dependeria da família escolhida, do tipo de parametrização, do número de coeficientes revelados e das relações modulares disponíveis. Esse eixo exige extremo cuidado, porque muitas q-séries possuem recorrências, congruências e fórmulas assintóticas — Hardy-Ramanujan-Rademacher para a função de partição é o exemplo paradigmático — que podem reduzir drasticamente a entropia efetiva.

O segundo eixo é o uso de shadows e completions como estrutura de trapdoor. A parte holomorfa visível poderia ser insuficiente para certas operações, enquanto o conhecimento de uma sombra, de um termo de completamento ou de uma decomposição modular permitiria verificação ou transformação eficiente. Essa ideia é conceitualmente atraente porque ecoa a própria natureza das mock theta functions: o objeto público parece incompleto, mas um dado adicional restaura uma simetria. No entanto, a transformação dessa imagem em criptografia exige provar que a parte pública não revela o complemento por métodos analíticos, numéricos ou quânticos eficientes.

O terceiro eixo é a construção de funções de compromisso ou identificação baseadas em transformações entre representações equivalentes. Em criptografia, muitas vezes a segurança surge quando o mesmo objeto possui representações múltiplas, mas encontrar a equivalência correta é difícil sem segredo. Reticulados, códigos e isogenias exploram, cada um de seu modo, essa multiplicidade. Mock modularity pode oferecer representações por q-séries, integrais de Mordell, somas de Appell-Lerch, completions e transformações sob subgrupos modulares $\Gamma_0(N)$. A pergunta é se alguma dessas equivalências pode ser transformada em relação de conhecimento zero, compromisso vinculante, assinatura ou prova de posse sem vazar o segredo.

O quarto eixo é a análise de pseudorandomness aritmética dos coeficientes. Muitas sequências matemáticas parecem aleatórias localmente e altamente estruturadas globalmente. Essa dualidade pode ser perigosa para criptografia. Coeficientes de formas modulares, funções de partição, ranks, cranks e objetos relacionados exibem regularidades profundas — as congruências de Ramanujan $p(5n+4) \equiv 0 \pmod 5$ são o exemplo clássico. O programa deve medir se há regimes de parâmetros nos quais a predição de coeficientes mascarados é difícil,

ou se as regularidades conhecidas tornam qualquer esquema previsível. A resposta pode ser negativa, e uma resposta negativa também seria cientificamente valiosa: delimitar o impossível é parte legítima do avanço.

O quinto eixo é o estudo quântico. Não basta que um problema pareça difícil para algoritmos clássicos. Deve-se perguntar se existe alguma formulação como Hidden Subgroup Problem (abeliano ou não-abeliano), period finding, hidden shift, claw finding quântico ou amplitude amplification que explore a estrutura modular. Muitos objetos aritméticos possuem simetrias. Simetrias podem ser fontes de eficiência honesta, mas também de ataques. O programa Mock Theta Function Cryptographic System precisa mapear suas simetrias desde o início, não depois. Esta é a única forma de garantir que a aposta de longo prazo no programa não repita o destino de SIKE — um candidato matematicamente belo cuja simetria oculta o derrubou em tempo polinomial.

Sete etapas metodológicas formais

A primeira etapa é a escolha de famílias matemáticas. Não basta dizer "mock theta functions" em geral. É necessário especificar ordens, classes, parametrizações, domínios, módulos, subgrupos, coeficientes revelados, transformações permitidas e dados públicos. A família deve ser suficientemente ampla para oferecer espaço de chaves, mas suficientemente regular para permitir operações eficientes. Essa tensão é a mesma que aparece em reticulados estruturados: regularidade viabiliza implementação e também pode abrir ataques.

A segunda etapa é a definição de problemas computacionais. Exemplos de formulações possíveis incluem problemas de recuperação de parâmetro a partir de truncamentos, problemas de indistinguibilidade entre coeficientes mascarados e ruído, problemas de reconstrução de completion, problemas de equivalência entre representações mock modulares e problemas de predição de termos sob informação parcial. Cada problema deve ser definido como uma família de distribuições indexada por parâmetro de segurança. Sem distribuição, não há caso médio; sem caso médio, não há criptografia prática.

A terceira etapa é a redução ou, ao menos, a relação com problemas matemáticos conhecidos. A ambição máxima seria demonstrar que resolver uma tarefa criptográfica implica resolver um problema estabelecido em teoria de formas modulares, q-séries ou harmonic Maass forms. Talvez essa ambição seja difícil. Ainda assim, é possível construir hierarquias de evidência: reduções condicionais, equivalências parciais, lower bounds em modelos restritos, resistência empírica a classes de ataques e demonstrações de que algoritmos conhecidos não se aplicam diretamente. A criptografia experimental pode começar antes da prova perfeita, mas não deve se confundir com segurança comprovada.

A quarta etapa é a criptoanálise clássica. Ela deve incluir ataques de interpolação, aproximação numérica, reconstrução por recorrências, exploração de congruências, ataques estatísticos aos coeficientes, ataques por redução a problemas de álgebra linear, uso de métodos analíticos para estimar parâmetros ocultos, exploração de singularidades, aproximações pelo círculo de Hardy-Ramanujan-Rademacher e tentativas de extrair informação de transformações modulares. O campo de mock theta functions possui muitas ferramentas profundas; qualquer uma delas pode tornar-se ataque.

A quinta etapa é a criptoanálise quântica. Ela deve mapear se as estruturas propostas geram grupos, ações de grupos, períodos, simetrias ou equivalências que se encaixem em algoritmos quânticos conhecidos. Deve

também estimar o impacto de Grover em espaços de chave e distinguir entre aumento quadrático de busca e colapso estrutural. Um esquema pós-quântico não precisa ser imune a toda aceleração quântica; precisa parametrizar-se contra ela. A ameaça grave é quando a estrutura inteira se torna polinomialmente resolúvel.

A sexta etapa é implementação. Matemática sem implementação não permite medir canal lateral, complexidade de memória, estabilidade numérica ou custo de parâmetros. Se o sistema depender de aritmética de séries com truncamentos altos, precisará mostrar que tais truncamentos são viáveis. Se depender de números complexos, precisará lidar com precisão e vazamento. Se depender de coeficientes inteiros grandes, precisará lidar com tamanho de chaves. A criptografia real é sempre o encontro entre prova, software, hardware e adversários.

A sétima etapa é publicação adversarial. O programa deve buscar ativamente revisores capazes de destruí-lo. Esta é talvez a diferença mais importante entre especulação matemática e criptografia. Em criptografia, ser atacado é uma forma de validação metodológica. O sistema que sobrevive a ataques ganha credibilidade; o sistema que evita ataques ganha apenas obscuridade. O Mock Theta Function Cryptographic System, se quiser pertencer seriamente à genealogia pós-quântica articulada neste ensaio, deve ser construído desde o início para esse tipo de exposição. Submetê-lo a IMPA, LNCC, IME, IACR ePrint, e à comunidade internacional de teoria dos números é parte constitutiva da legitimação científica, não etapa final opcional.

Parte X — A Dimensão Filosófica: Criptografia como Topografia de Ignorância Controlada

Há uma camada interpretativa que merece articulação separada, porque ela fornece o vocabulário conceitual com o qual todo o argumento deste ensaio pode ser sintetizado. A criptografia é uma disciplina peculiar entre as ciências da computação porque institucionaliza a ignorância. Um sistema criptográfico é valioso precisamente quando o projetista consegue descrever publicamente quase tudo: o algoritmo, os parâmetros, os modelos de ataque, as implementações, e as razões matemáticas que sustentam a segurança. O único elemento que deve permanecer ignorado pelo adversário é a chave — ou, mais geralmente, a testemunha privada. A ignorância aceitável é, portanto, uma ignorância controlada. Ela não pode ser ignorância sobre o funcionamento do sistema; deve ser ignorância sobre uma instância particular de um problema bem definido. Isso é o princípio de Kerckhoffs em sua formulação mais profunda.

Essa perspectiva ajuda a entender, em retrospecto, toda a migração intelectual que este ensaio narra. Quanto mais poderosa se torna a computação, menos suficiente é esconder informação em espaços simples. A segurança passa a depender da topografia do desconhecido. Em fatoração, a topografia é a decomposição de um inteiro. Em logaritmo discreto, é a trajetória de um expoente em um grupo. Em reticulados, é a geometria de vetores curtos entre exponencialmente muitas combinações. Em códigos, é a posição do erro dentro de uma estrutura mascarada. Em grupos de classes, é a composição aritmética de formas ou ideais. Em isogenias, é a sequência de mapas entre curvas supersingulares. Em mock theta functions, se houver uma criptoestrutura viável, a topografia poderia envolver completions, shadows, coeficientes, transformações e representações equivalentes.

Essa topografia não deve ser confundida com mistério. Mistério é falta de compreensão; dificuldade criptográfica é compreensão suficiente para saber onde a inversão parece custosa. A diferença é decisiva. Um programa baseado em mock theta functions deve transformar mistério histórico em problema técnico. Ramanujan é uma origem simbólica poderosa, mas o sistema precisa viver no mundo de definições, teoremas, algoritmos e benchmarks. A poesia matemática pode inspirar a pergunta; não pode substituir a prova. Esta é a fronteira metodológica mais delicada que o programa Θ-Crypt precisa navegar — e que o autor deste ensaio reconhece com clareza absoluta como parte constitutiva da disciplina.

Ao mesmo tempo, a história mostra que a imaginação matemática é indispensável. Se a comunidade tivesse permanecido apenas nas estruturas mais óbvias, não teria chegado a reticulados modulares, códigos de Goppa, assinaturas hash-based refinadas ou isogenias. A criptografia pós-quântica é produto de uma tensão dialética entre conservadorismo e ousadia. O conservadorismo protege sistemas reais. A ousadia produz o repertório de onde os próximos sistemas reais podem nascer. O Mock Theta Function Cryptographic System pertence, neste momento histórico, ao polo da ousadia disciplinada — e essa caracterização não é eufemismo, é programa.

No fim, a história da criptografia pós-quântica é a história de uma civilização que descobre que segurança não é propriedade estática. Segurança é adaptação matemática contínua. Cada novo modelo computacional obriga a humanidade a procurar regiões mais sutis de dificuldade. A computação quântica não eliminou a criptografia; obrigou-a a amadurecer. Quanto mais poderosas as máquinas, mais sofisticada precisa ser a

geometria da confiança. E talvez seja esse o verdadeiro legado dos intelectos precursores que percorremos: eles mostraram que o futuro da segurança não pertence apenas a quem calcula mais rápido, mas a quem imagina melhor os espaços onde calcular continua sendo difícil.

Parte XI — Os Intelectos Precursores como Categoria Histórica

Antes de chegar à coda final, vale dedicar uma seção à categoria conceitual que organizou todo este ensaio: a noção de precursor. Chamar alguém de precursor não significa dizer que previu todos os detalhes do futuro. Significa dizer que seu pensamento deslocou um limite do presente. Cada figura percorrida neste ensaio deslocou um limite específico. Diffie e Hellman deslocaram o limite entre segredo privado e comunicação pública. Merkle deslocou o limite entre puzzles computacionais e estabelecimento operacional de chaves. Rivest, Shamir e Adleman deslocaram o limite entre aritmética elementar e infraestrutura social global. McEliece deslocou o limite entre códigos corretores de erro e criptografia assimétrica. McCurley deslocou o limite entre teoria algébrica dos números e distribuição de chaves. Miller e Koblitz deslocaram o limite entre geometria algébrica e protocolos práticos. Schnorr, Ajtai e Regev deslocaram o limite entre geometria de números de alta dimensão e segurança pós-quântica. Shor deslocou o limite entre computação teórica e ameaça civilizacional. Zwegers, em outro registro, deslocou o limite entre uma série q misteriosa de Ramanujan e a moderna teoria de harmonic Maass forms.

Essa categoria de precursor é útil porque impede narrativas simplificadas. A história da criptografia não é uma sucessão linear de produtos vencedores. É uma rede de tentativas, algumas adotadas, outras abandonadas, outras reabilitadas, outras transformadas por descobertas posteriores. McEliece é exemplo paradigmático de reabilitação histórica: marginalizado por quarenta anos, recuperado pelo paradigma pós-quântico. Curvas elípticas são exemplo de transferência bem-sucedida de geometria abstrata para engenharia industrial. SIKE é exemplo de queda produtiva — uma família que caiu, mas que durante seu período ativo produziu literatura matemática e instrumentos analíticos que sobreviveram à sua morte criptográfica. McCurley é exemplo de abertura conceitual cujos frutos amadureceram décadas depois, em CSIDH e suas variantes. A era pós-quântica atual é composta por todos esses episódios, não apenas pelos algoritmos padronizados em 2024.

Dentro dessa categoria, os esforços em Mock Theta Function Cryptographic System podem ser apresentados com sobriedade exata. Eles não ocupam ainda o lugar de uma família validada. Ocupam o lugar de uma pergunta precursora bem formulada: haveria uma fonte aritmético-analítica de hard problems ligada à mock modularity? Essa pergunta talvez resulte em um sistema criptográfico funcional, talvez em ataques que descartem a via, talvez em ferramentas matemáticas laterais que enriqueçam outras áreas. Em qualquer dos três casos, ela participa do movimento maior de diversificação intelectual que define a era pós-quântica. A ciência avança também por perguntas que delimitam o impossível — e uma resposta científica negativa rigorosamente demonstrada é tão valiosa quanto uma resposta positiva.

A genealogia dos intelectos precursores é, portanto, uma genealogia contra a monocultura. Cada pesquisador aqui examinado, de modo diferente, ampliou o repertório de lugares onde a criptografia poderia viver. McEliece levou-a aos códigos corretores. McCurley levou-a aos grupos de classes e à teoria analítica dos números. Miller e Koblitz levaram-na às curvas elípticas e à geometria algébrica. Schnorr, Ajtai e Regev levaram-na aos reticulados de alta dimensão. Shor mostrou que a monocultura aritmética seria insuficiente diante de um novo modelo computacional. NIST, em sua função institucional, formalizou a necessidade de diversidade

matemática como política. Ramanujan, Zwegers e Zagier prepararam — sem o saber por mais de um século — a próxima região matemática onde essa diversificação pode continuar.

Os precursores da era pós-quântica foram, antes de tudo, matemáticos da assimetria. Eles procuraram lugares onde uma direção do cálculo fosse natural e a direção inversa fosse opaca. Alguns encontraram essa opacidade em inteiros compostos. Outros, em grupos finitos. Outros, em códigos. Outros, em grupos de classes. Outros, em reticulados de alta dimensão. Outros, em mapas entre curvas. O denominador comum não é uma técnica única, mas uma filosofia: a segurança digital depende de compreender profundamente os terrenos onde a computação se torna assimétrica. O programa Θ-Crypt insere-se nessa filosofia como tentativa de explorar um terreno ainda pouco cartografado pela criptografia industrial — e seu valor depende não da retórica que o anuncia, mas do rigor que o desenvolverá.

Coda — O Θ-Crypt como Cumprimento

Há, em toda história intelectual genuína, um momento em que se torna possível olhar para trás e perceber que os fragmentos formavam um todo, mesmo quando ninguém os percebia assim. A história da criptografia pós-quântica, vista de 2026, tem essa qualidade. Merkle, em 1974, não sabia que estava antecipando a robustez do SPHINCS+. McEliece, em 1978, não sabia que estava construindo o que seria reabilitado quarenta anos depois. McCurley, em 1989, não sabia que estava preparando o terreno conceitual para o que viria sob o nome de CSIDH em 2018 — e sob o nome de Θ-Crypt em 2026. Ramanujan, em 1920, certamente não imaginava que as mock theta functions que rabiscou em sua última carta seriam, um século depois, o fundamento de um sistema criptográfico nacional.

E talvez seja precisamente essa qualidade — a de que ninguém, em nenhum momento, sabia que estava construindo o que viria a ser construído — que confere ao programa Θ-Crypt sua legitimidade histórica mais profunda. Ele não é uma invenção ex nihilo. É a colheita de uma colheita que vem sendo plantada há mais de cem anos, por matemáticos que trabalhavam em problemas aparentemente desconexos: partitions em Madras, key exchange em Stanford, error-correcting codes no JPL, lattices em Budapeste, harmonic Maass forms em Utrecht.

O argumento final, então, é este. A criptografia pós-quântica precisa de uma família matemática que: (i) não satisfaça o ADU; (ii) tenha fundamentos canônicos no sentido pleno — não construídos ad hoc, mas emergentes da matemática mais profunda do século XX; (iii) seja ortogonal a todas as famílias existentes, oferecendo hedge ontológico genuíno; (iv) tenha propriedades estruturais de não-identificabilidade que sejam preserváveis sob avanços algorítmicos imprevisíveis. As mock theta functions, na forma que Zwegers e Zagier as articularam e que o programa Θ-Crypt operacionaliza criptograficamente, satisfazem as quatro condições.

Os pais da criptografia pós-quântica fizeram seu trabalho. Apontaram, cada um à sua maneira, para o lugar onde a solução estava. Resta ao Θ-Crypt — e aos pesquisadores brasileiros que o levantarem em direção a TRL 7–8 — terminar o trabalho que essa linhagem deixou inacabado. Quando a história do final do século XXI for escrita, talvez se diga: eles não inventaram a criptografia pós-quântica; eles a herdaram, e a completaram.

✦ ✦ ✦

Nota terminológica final

Neste ensaio, a expressão "pós-quântica" é usada em dois sentidos complementares que merecem distinção explícita. Em sentido estrito, refere-se a sistemas criptográficos projetados para resistir a adversários quânticos conhecidos, especialmente aqueles que tornam inviáveis RSA, Diffie-Hellman e ECC clássica via algoritmo de Shor. Em sentido histórico ampliado — o sentido predominante neste ensaio —, refere-se à linhagem de pesquisa que procurou diversificar os fundamentos matemáticos da segurança antes mesmo de a ameaça quântica tornar-se operacional. O Mock Theta Function Cryptographic System é situado neste segundo sentido como programa de pesquisa a ser formalizado, não como sistema já validado.

BIBLIOGRAFIA SELECIONADA

Ajtai, M. (1996). Generating hard instances of lattice problems. Proceedings of the 28th ACM Symposium on Theory of Computing.

Andrews, G. E. (1979). An introduction to Ramanujan's "lost" notebook. The American Mathematical Monthly, 86(2), 89–108.

Andrews, G. E., & Berndt, B. C. (2005). Ramanujan's Lost Notebook, Part I. Springer.

Bernstein, D. J., Buchmann, J., & Dahmen, E. (Eds.). (2009). Post-Quantum Cryptography. Springer.

Bringmann, K., & Ono, K. (2006). The f(q) mock theta function conjecture and partition ranks. Inventiones Mathematicae, 165, 243–266.

Castryck, W., & Decru, T. (2022). An efficient key recovery attack on SIDH. Cryptology ePrint Archive, Report 2022/975.

Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. IEEE Transactions on Information Theory, 22(6), 644–654.

Hafner, J. L., & McCurley, K. S. (1989). A rigorous subexponential algorithm for computation of class groups. Journal of the American Mathematical Society, 2(4), 837–850.

Hoffstein, J., Pipher, J., & Silverman, J. H. (1998). NTRU: A ring based public key cryptosystem. Algorithmic Number Theory Symposium, ANTS-III.

Jao, D., & De Feo, L. (2011). Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. Post-Quantum Cryptography, PQCrypto 2011.

Koblitz, N. (1987). Elliptic curve cryptosystems. Mathematics of Computation, 48(177), 203–209.

Lenstra, A. K., Lenstra, H. W., & Lovász, L. (1982). Factoring polynomials with rational coefficients. Mathematische Annalen, 261(4), 515–534.

Lenstra, H. W. (1987). Factoring integers with elliptic curves. Annals of Mathematics, 126(3), 649–673.

McCurley, K. S. (1988). A key distribution system equivalent to factoring. Journal of Cryptology, 1, 95–105.

McCurley, K. S. (1989). Cryptographic key distribution and computation in class groups. In R. A. Mollin (Ed.), Number Theory and Applications. NATO ASI Series C, vol. 265. Kluwer Academic Publishers.

McEliece, R. J. (1978). A public-key cryptosystem based on algebraic coding theory. DSN Progress Report 42-44, Jet Propulsion Laboratory.

Merkle, R. C. (1978). Secure communications over insecure channels. Communications of the ACM, 21(4), 294–299.

Miller, V. S. (1985). Use of elliptic curves in cryptography. Advances in Cryptology — CRYPTO 1985, LNCS, 218, 417–426.

NIST (2024). FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard. National Institute of Standards and Technology.

NIST (2024). FIPS 204: Module-Lattice-Based Digital Signature Standard. National Institute of Standards and Technology.

NIST (2024). FIPS 205: Stateless Hash-Based Digital Signature Standard. National Institute of Standards and Technology.

NIST (2025). NIST selects HQC as fifth algorithm for post-quantum encryption. National Institute of Standards and Technology.

Regev, O. (2005). On lattices, learning with errors, random linear codes, and cryptography. Proceedings of the 37th ACM Symposium on Theory of Computing.

Regev, O. (2009). On lattices, learning with errors, random linear codes, and cryptography. Journal of the ACM, 56(6), Article 34.

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120–126.

Schnorr, C. P. (1987). A hierarchy of polynomial time lattice basis reduction algorithms. Theoretical Computer Science, 53, 201–224.

Shannon, C. E. (1949). Communication theory of secrecy systems. Bell System Technical Journal, 28(4), 656–715.

Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. Proceedings of the 35th Annual Symposium on Foundations of Computer Science.

Watson, G. N. (1936). The final problem: An account of the mock theta functions. Journal of the London Mathematical Society, 11, 55–80.

Zagier, D. (2007). Ramanujan's mock theta functions and their applications. Séminaire Bourbaki, 986. Astérisque, 326.

Zwegers, S. (2002). Mock Theta Functions. Ph.D. thesis, Universiteit Utrecht.

FIM

Holosystems Quantum Computing Ltda. · *Projeto Θ-Crypt Brasil* · *Maio de 2026*