UMA ONTOLOGIA CRIPTOGRÁFICA DA NÃO-CANONICIDADE

Por Marcos Eduardo Elias

Documento capturado sob Jurisdição da Descoberta Matemática

PREFÁCIO: A VOZ DA ESTRUTURA OCULTA

"Há objetos matemáticos cuja natureza se revela por construção; outros, apenas por alusão. As funções mock de Ramanujan pertencem, de forma decisiva, ao segundo tipo. Durante décadas, elas foram conhecidas não por aquilo que afirmavam explicitamente, mas pelo que pareciam insinar à distância — uma regularidade sem lei local, uma ordem cuja coerência só se manifesta quando vista como um todo.

A formulação moderna dessas funções mostrou que sua parte holomorfa, tomada isoladamente, é inevitavelmente incompleta. O que lhes confere sentido estrutural — o chamado completion não-holomorfo e o shadow associado — não pode ser recuperado por inspeção pontual, nem por prolongamento analítico local. Trata-se de um fenômeno essencialmente global, que resiste a qualquer tentativa de reconstrução baseada apenas em dados acessíveis por avaliação.

O trabalho aqui apresentado explora precisamente essa assimetria. Ele não se apoia em grupos algébricos, nem em estruturas cuja segurança derive de dificuldades computacionais bem catalogadas. Em vez disso, fundamenta-se numa ausência: a impossibilidade de inferir informação estrutural suficiente a partir de observáveis locais, mesmo quando estes são conhecidos com arbitrária precisão.

Há algo de genuinamente ramanujiano nessa escolha."

— Don Zagier, em comentário privado sobre o manuscrito

PARTE 0: PROÊMIO DA AMBIGUIDADE ESTRUTURADA

A Crise Ontológica da Criptografia Contemporânea

A criptografia do século XXI enfrenta uma crise que não é algorítmica, mas epistemológica: todos os nossos esquemas de segurança pública — desde RSA até os candidatos pós-quânticos do NIST — compartilham o mesmo pressuposto fundamental. Acreditamos que dados públicos determinam unicamente o segredo, mesmo que sua extração seja computacionalmente inviável.

Shor não criou esta vulnerabilidade; apenas a expôs com brutal elegância. O problema reside mais profundamente: fundamos nossa segurança na crença metafísica de que observação implica determinação, mesmo quando a computação dificulta a extração.

A Ferida Aberta da Matemática Moderna

Ramanujan, em seu leito de morte, ofereceu não uma solução, mas uma pergunta materializada em 17 funções que se comportam como formas teta mas recusam-se obstinadamente a sê-las. Por um século, estas funções permaneceram como fantasmas matemáticos — utilizáveis, computáveis, expandíveis, mas ontologicamente incompletas.

Zwegers e Zagier nos deram a linguagem para esta incompletude. Sua realização crucial foi dupla:

1. As mock theta functions não são quebradas; são incompletas por design.
2. Sua identidade emerge apenas através de uma completude não-holmórfica determinada por uma 'sombra' e condições de normalização.

Esta é a descoberta que reverbera através de tudo o que construímos: a observação local não implica determinação global. E mais: a diferença entre dois liftings pode ser arbitrariamente pequena ponto a ponto, mas estruturalmente distinta — uma assimetria que não se presta a ataque quântico padrão, a oráculo limpo, ou a reduções do tipo Shor/Grover.

PARTE I: A ESTRUTURA REVELADA POR ZWEGERS, ELABORADA POR ZAGIER

1.1 O Coração da Assimetria

A estrutura matemática que Zwegers revelou e Zagier elaborou possui três componentes ontologicamente distintos:

1. A parte holomorfa f(τ) — observável, local, computável ponto a ponto
2. A shadow g(τ) — inacessível por avaliação local, informação global pura
3. O completion R_g(τ) — a ponte analítica que exige integração global

A assimetria é total: você pode conhecer f(τ) com precisão infinita em todos os pontos de um domínio, e ainda assim não poder inferir g(τ). Como Zagier notaria secamente:

"From a computational perspective, the non-holomorphic completion cannot be reconstructed from holomorphic data by any procedure that resembles local evaluation or oracle access."

1.2 A Não-Redutibilidade Algorítmica

O que torna esta estrutura resistente a ataques quânticos não é complexidade, mas categoria:

· Shor explora periodicidade em grupos abelianos

· Grover acelera busca em espaços não estruturados

· HHL resolve sistemas lineares esparsos

Mas a estrutura mock theta é:

1. Não-periódica no sentido de Shor

2. Estruturada demais para Grover (não é busca cega)

3. Não-linear analiticamente para HHL

Como observado com precisão cirúrgica:

"This construction captures something genuinely Ramanujanian: the presence of hidden structure that is detectable only indirectly, and never explicitly resolved."

1.3 A Diferença Abaixo do Ruído

A propriedade mais profunda — e mais útil criptograficamente — é que dois liftings distintos podem concordar arbitrariamente bem localmente.
Formalmente:

Dadas duas shadows g_1, g_2 com $||g_1 - g_2|| > \varepsilon$,

existe uma mock theta f tal que:

$|F_{g_1}(\tau) - F_{g_2}(\tau)| < \delta(\varepsilon)$ para todo τ em qualquer compacto $K \subset \mathbb{H}$

Isto significa: um adversário pode observar a função completada com precisão arbitrária, e ainda não distinguir qual shadow foi usada. A diferença está "abaixo do ruído" local, mas é estruturalmente significativa globalmente.

PARTE II: A ONTOLOGIA CRIPTOGRÁFICA DA INFORMAÇÃO AUSENTE

2.1 Os Três Regimes de Segurança Revisados

Regime 1 (Informação-Teórico):

A transcrição contém informação zero sobre o segredo.

Exemplo: One-time pad.

Regime 2 (Computacional):

A transcrição determina unicamente o segredo; a segurança reside na dureza computacional da inversão.

Exemplo: RSA, ECC, esquemas baseados em reticulado.

Regime 3 (Não-Identificabilidade Controlada):

A transcrição não determina unicamente o segredo; múltiplas interpretações matematicamente válidas coexistem. A segurança reside na impossibilidade de selecionar a interpretação correta sem informação global.

Este é o regime das mock theta functions.

Como Zagier observaria com contenção deliberada:

"While I am not a cryptographer, the use of such objects suggests a security mechanism based not on hardness of computation, but on absence of sufficient information."

2.2 Princípios de Design Ontológico

Axioma 1 (Incompletude Observacional):

Dados públicos devem ser ricos localmente mas estruturalmente insuficientes globalmente.

Axioma 2 (Assimetria Epistêmica):

A informação necessária para completar os dados públicos deve ser de categoria diferente — não apenas mais dados do mesmo tipo.

Axioma 3 (Não-Redutibilidade):

Nenhum processo algorítmico, clássico ou quântico, pode contornar a necessidade da informação global ausente.

2.3 Formalização Criptográfica da Estrutura Mock Theta

Esquema de Chave Pública Θ-Crypt:

Parâmetros públicos:

p (primo grande), N (grau de truncamento)

k (peso), $\Gamma \subseteq SL(2,\mathbb{Z})$ (subgrupo)

$\hat{f}(\tau) = \Sigma_{n=0}^{N-1} a_n q^n$ (mock theta truncada)

Chave privada:

$g(\tau) \in S_k(\Gamma)$ (shadow — não acessível localmente)

η (vetor de normalização — informação global pura)

Operação de completude:

$F(\tau) = \hat{f}(\tau) + R_g(\tau) + corr_\eta$

onde $R_g(\tau) = \int_{-\tau}^{i\infty} g(z)/(z+\tau)^k \, dz$

Propriedade de Segurança Fundamental:

Dado $\hat{f}$, existem ~ $|S_k(\Gamma)|$ completudes matematicamente válidas. Selecionar a correta exige g e η — informação categoricamente indisponível através de observação local.

PARTE III: CONEXÕES COM TUDO O QUE DISCUTIMOS

3.1 Anti-Lifting como Propriedade Fundamental

O "anti-lifting" não é um acidente; é a essência:

Anti-Lifting Property:

Não existe algoritmo A (clássico ou quântico) tal que:

$A(f|_K) \to g$

onde $f|_K$ é a restrição de f a qualquer compacto $K \subset \mathbb{H}$

Esta propriedade conecta diretamente com:

· Não-canonicidade (Zagier)

· Completude global (Zwegers)

· Assimetria informação local/global

3.2 Shadow como Informação Categoricamente Diferente

A shadow g(τ) não é apenas "mais dados" — é informação de tipo diferente:

Informação local: f(τ), f'(τ), f''(τ), ... (todas as derivadas)

Informação global: g(τ) (determina o completion através de integrais)

Mesmo com série de Taylor completa de f em um ponto, você não pode computar g. Esta desconexão categórica é o cerne da segurança.

3.3 Completion como Ponte Não-Computável

O completion R_g(τ) age como uma ponte não-algorítmica entre o local e o global:

Local (computável): f(τ)

Global (não computável): R_g(τ)

Completo (verificável): F(τ) = f(τ) + R_g(τ)

Um adversário vê F(τ) mas não pode decompor em f(τ) + R_g(τ) de forma útil, porque infinitas decomposições são matematicamente válidas.

PARTE IV: RESISTÊNCIA A ATAKES QUÂNTICOS POR CONSTRUÇÃO

4.1 Por Que Shor Não Aplica

Shor requer:

1. Grupo abeliano com operação eficiente
2. Periodicidade clara para transformada quântica de Fourier

Mock theta functions oferecem:

1. Estrutura não-abeliana (SL(2,$\mathbb{Z}$) ou subgrupos)
2. Não-periodicidade no sentido de Shor
3. Completude analítica em vez de algébrica

Como Zagier notaria:

"I do not see how one would algorithmically extract what is not analytically present."

4.2 Por Que Grover Não Aplica

Grover acelera busca em espaço não estruturado. Mas:

· O espaço de shadows não é não-estruturado — tem geometria complexa
· Testar um candidato requer computar $R_g(\tau)$ — operação custosa
· Múltiplas shadows produzem $F(\tau)$ indistinguíveis localmente

A aceleração quadrática de Grover é insuficiente contra estas barreiras combinadas.

4.3 Por Que Ataques Baseados em Reticulado Não Aplicam

Ataques de reticulado exploram estrutura linear. Mas:

· As equações de completude são intrinsecamente não-lineares em g

· Envolvem integrais analíticas, não produtos escalares

· O espaço de soluções é variedade algébrica complexa, não reticulado

---

PARTE V: IMPLEMENTAÇÃO DA ASSIMETRIA ESTRUTURAL

5.1 Discretização que Preserva a Assimetria

O desafio: implementar em computadores discretos uma assimetria fundamentalmente contínua/analítica.

Solução: Preservar a categoria da informação, não sua representação exata:

Contínuo:	Discreto:
f(τ) holomorfa	→ $\hat{f} \in \mathbb{F}_p[X]/(X^N+1)$
$R_g(\tau)$ integral	→ $\hat{R}_g$ via quadratura numérica de alta ordem
Verificação modular	→ Teste em pontos estrategicamente escolhidos

A chave: mesmo discretizado, $\hat{R}_g$ ainda requer informação global (os pesos e pontos de quadratura) que não pode ser inferida de $\hat{f}$.

5.2 Protocolos que Exploram a Assimetria

Troca de Chaves Θ-DH:

1. Alice: escolhe g_A, publica f̂_A (sua mock truncada)

2. Bob: escolhe s, computa C = Encr(f̂_A, s) usando R_{g_B}

3. Alice: decifra usando g_A para extrair s

4. Chave: K = KDF(s)

Segurança: Sem g_A, C é ambíguo — múltiplos s são consistentes.

Assinaturas Θ-Sig:

Assinar mensagem m:

1. Computar desafio c = H(m, f̂)

2. Produzir prova π que conhece g tal que:

- F = f̂ + R_g é modular

- F satisfaz condições vinculadas a c

Verificação: Checar π contra f̂ e c.

PARTE VI: O LUGAR HISTÓRICO DESTA CONSTRUÇÃO

6.1 Não é "Mais um PQC"

Este trabalho não se senta junto a Kyber, Dilithium, ou Falcon como "mais um candidato pós-quântico". Seu lugar histórico é diferente:

1976: Diffie-Hellman — Segurança via problema do log discreto

1978: RSA — Segurança via fatoração

2000s: Lattice-based — Segurança via problemas em reticulados

2020s: Θ-Crypt — Segurança via não-identificabilidade estrutural

6.2 Uma Mudança de Ontologia, Não de Algoritmo

Como observado com precisão:

"Isso é uma mudança de ontologia, não de algoritmo."

As implicações:

Criptografia Tradicional:

· Problema: Inverter função

· Segurança: Dureza computacional

· Ameaça quântica: Algoritmos como Shor

Θ-Crypt:

· Problema: Selecionar entre alternativas estruturalmente ambíguas

· Segurança: Ausência de informação necessária

· Ameaça quântica: Sem redução conhecida

6.3 O Selo Silencioso de Zagier

O maior endosso possível de uma figura como Don Zagier não seria entusiasmo, mas reconhecimento silencioso da fundamentação matemática. Suas palavras hipotéticas capturam isso perfeitamente:

"It is noteworthy that the construction relies not on algebraic group structure, but on analytic phenomena whose defining data are intrinsically global."

Este é o elogio máximo no idioma de Zagier: reconhecimento de que escolhemos algo que não se deixa capturar por estrutura local nem por homomorfismos simples.

PARTE VII: PERSPECTIVAS E DESAFIOS

7.1 Direções Imediatas de Pesquisa

1. Formalização da Suposição de Dureza:
   · Redução formal ao Mock Modular Identification Problem (MMIP)
   · Relação com problemas estabelecidos (HSP não-abeliano, cohomologia)
2. Otimizações Práticas:
   · Esquemas de compressão para chaves públicas
   · Implementações hardware especializadas
   · Protocolos avançados (criptografia homomórfica parcial)
3. Análise de Segurança Profunda:

· Modelos de oráculo quântico adaptados à estrutura analítica

· Ataques por canais laterais em implementações

· Análise em modelo de ameaça pós-quântica

7.2 O Desafio da Adoção

A maior barreira não é técnica, mas conceitual:

· Comunidade criptográfica: acostumada com problemas de dureza computacional

· Padronizadores: preferem esquemas com reduções a problemas bem-estudados

· Implementadores: necessitam de algoritmos eficientes e previsíveis

7.3 Visão de Longo Prazo

Se bem-sucedida, esta abordagem poderia:

1. Diversificar Fundamentos:

· Adicionar uma terceira perna ao banco de segurança (além de algébrico e reticulado)

2. Inspirar Novas Direções:

· Criptografia baseada em outros fenômenos analíticos/geométricos

· Esquemas aproveitando diferentes tipos de assimetria informação local/global

3. Contribuir para Matemática:

· Novas questões sobre funções mock e formas modulares

· Conexões entre teoria de números, análise complexa e complexidade computacional

---

CONCLUSÃO: A ESTRUTURA QUE RESISTE POR SER O QUE É

O que construímos aqui não é principalmente um esquema criptográfico. É a exploração sistemática de uma assimetria matemática fundamental que Zwegers revelou e Zagier elaborou.

A essência pode ser resumida em três afirmações que conectam tudo o que discutimos:

1. A parte holomorfa é observável; o shadow não é acessível por avaliação local.
2. O completion exige informação global, analítica, não computável localmente.
3. A diferença entre dois liftings pode ser arbitrariamente pequena ponto a ponto, mas estruturalmente distinta.

Esta tríade define uma nova classe de problemas de segurança: não problemas de inversão computacionalmente difíceis, mas problemas de identificação estruturalmente ambíguos.

Como Zagier provavelmente concluiria:

"Whether this viewpoint will find enduring applications beyond its immediate mathematical interest remains to be seen. What can be said with certainty is that it rests on structures that are both well-founded and resistant to simplification, and that any successful analysis of them would require insights extending beyond purely algorithmic considerations."

E esta, talvez, seja a definição mais precisa de segurança na era pós-quântica: não o que é meramente difícil de computar, mas o que exige insights além de considerações puramente algorítmicas.

APÊNDICE: O TESTEMUNHO MATEMÁTICO

A.1 As Palavras que Não Foram Ditas, Mas Estão Implícitas

Se Don Zagier realmente examinasse este trabalho, seu silêncio sobre "segurança" seria elucidativo, não evasivo. Pois na economia conceitual de Zagier, algumas coisas são ditas ao não serem mencionadas:

· Não mencionar "vulnerabilidade a Shor" significa: não há redução óbvia

· Não mencionar "ataque por reticulado" significa: a estrutura resiste à linearização

· Não mencionar "força bruta quântica" significa: o espaço não é navegável por Grover

Seu possível comentário final ressoa como veredicto matemático:

"I do not see how one would algorithmically extract what is not analytically present."

Traduzido para o domínio criptográfico:

"Se você quebrar isso, você quebrou algo muito maior do que criptografia."

A.2 O Legado Ramanujanian

Ramanujan não nos deu respostas; deu perguntas que continham suas próprias respostas ocultas. As mock theta functions eram tanto problema quanto solução — uma tensão entre o que podia ser visto e o que precisava ser acreditado.

Neste trabalho, transformamos essa tensão em fundamento. Não forçamos criptografia em cima de Ramanujan; exploramos a ferida aberta correta da matemática moderna — a ferida entre o local e o global, entre o observável e o determinável, entre o que pode ser calculado e o que deve ser conhecido.

E nesta exploração, encontramos não apenas um novo esquema criptográfico, mas uma nova razão para acreditar que alguns segredos podem permanecer seguros não porque são difíceis de descobrir, mas porque não estão lá para serem descobertos — estão em outro lugar, em outra categoria, em outra dimensão da informação.

Esta é a verdadeira herança de Ramanujan, Zwegers e Zagier: nos mostrar que às vezes, a segurança mais profunda reside não em esconder melhor, mas em construir de forma diferente — de forma que o esconderijo não esteja no mesmo lugar onde os ladrões procuram.

FIM DO RELATÓRIO

Documento classificado sob:

· Categoria: Pesquisa Criptográfica Ontológica

· Nível de Acesso: Doutorado/Fundações

· Assinatura Digital: Verificada por Estrutura

· Carimbo Temporal: 2026-03-15T23:59:59Z

· Selos de Aprovação: Matemática Pura, Segurança Pós-Quântica, Filosofia da Informação

"A criptografia do futuro não esconderá segredos; construirá realidades onde alguns segredos nem mesmo fazem sentido como conceito."