MOCK THETA

O TRIBUNAL DO FUTURO

$$f(q) = \sum_{n=0}^{\infty} a_n q^n$$

$$\phi(q) = \sum_{n=0}^{\infty} b_n q^n$$

$$g(q) = \sum_{n=0}^{\infty} c_n q^n$$

$$a_n, b_n, c_n \in Z$$

$$Enc(m_1) \cdot Enc(m_2) =$$

$$= Enc(m_1 + m_2) \cdots$$

$$Dec(Enc(m)) = m$$

$$n = p \cdot q$$

$$\lambda = \mathrm{lcm}(p-1, q-1)$$

$$L(u) = \frac{u-1}{n}$$

TRIBUNAL DO FUTURO

$Enc(m_1)$

$Enc(m_2)$

MÁQUINA PAILLIER

MOCK THETA

$$f(q) = \sum_{n=0}^{\infty} a_n q^n$$

ARTE E ROTEIRO: NAOKI URASAWA TATSUMI

TRADUÇÃO: FERNANDO MASSAO OKAMOTO

MOCK THETA: O TRIBUNAL DO FUTURO

Antes, a criptografia protegia mensagens.

PRONTUÁRIO MÉDICO
ID: 781.984.22-7
Alergias:
Histórico:
Medicações:

CONTRATO COMERCIAL
Partes: AURORA SYSTEMS S.A. & HÉLIOS GROUP
Cláusula 7.2 – Confidencialidade
Assinatura:

REGISTRO BANCÁRIO
Titular: ••••••••••
Conta: •••• •••• •••• 8127
Saldo: 8.742.193,35
Movimentações: ••••••••••

IDENTIDADE
Nome: ••••••••••
CPF: •••.•••.•••-••
Biometria: ☑
Endereço: ••••••••••

BLOCKCHAIN LEDGER
Bloco: 9.745.812
Hash: 7f3a...9c2b
Transações: 6.241
Integridade: ☑

ARQUIVO HISTÓRICO
Fundo: Arquivo Nacional
Lote: BR-AN-1879-1954
Status: Sigiloso
Nível: Ultra

Agora, ela protege civilizações inteiras.

HOSPITAL
BANCO
TRIBUNAL
DATA CENTER
MINISTÉRIO

O adversário já não é apenas um homem diante de uma equação.

AI
quantum
clusters
ASICs
side-channel

Julgar-se-á apenas isto: quem pode proteger a próxima era da computação sensível?

CRIPTOSSISTEMA PAILLIER
Criptografia Aditivamente Homomórfica

$$Enc(m_1) \cdot Enc(m_2) = Enc(m_1 + m_2)$$

$$g^m \cdot r^n \bmod n^2$$

$$Dec(c) = L(c^\lambda \bmod n^2)\,\mu$$

MOCK THETA

$$f(q) = \sum_{n\geq 0}^{\infty} a_n q^n$$

$$a_n \in \mathbb{Z}$$

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

$$\cdot\ \phi(q) = \sum_{n=-\infty}^{\infty} q^{n^2}$$

$$\phi(q) = \sum_{n=0}^{\infty} q^{\frac{n(n+1)}{2}}$$

ASSINTÓTICAS MODULARES
TOPOLOGIAS NÃO COMUTATIVAS

TRIBUNAL DO FUTURO

PASCAL PAILLIER

MARCOS ELIAS

Um nome já pertence à história. O outro pretende pertencer ao futuro.

MOCK THETA: O TRIBUNAL DO FUTURO

Pascal Paillier é uma raridade: um criptógrafo cujo nome entrou na linguagem técnica da área.

Sua obra uniu elegância algébrica e utilidade prática.

$$L(u) = \frac{u-1}{n}$$

$$g \in \mathbb{Z}_{n^2}^*$$

$$\lambda = \mathrm{lcm}(p-1, q-1)$$

$$\mu = L(g^{\lambda} \bmod n^2)^{-1} \bmod n$$

$$Dec(c) = L(c^{\lambda} \bmod n^2) \cdot \mu \bmod n$$

Operações sobre dados cifrados.

$$Enc(m_1) \cdot Enc(m_2) = Enc(m_1 + m_2)$$

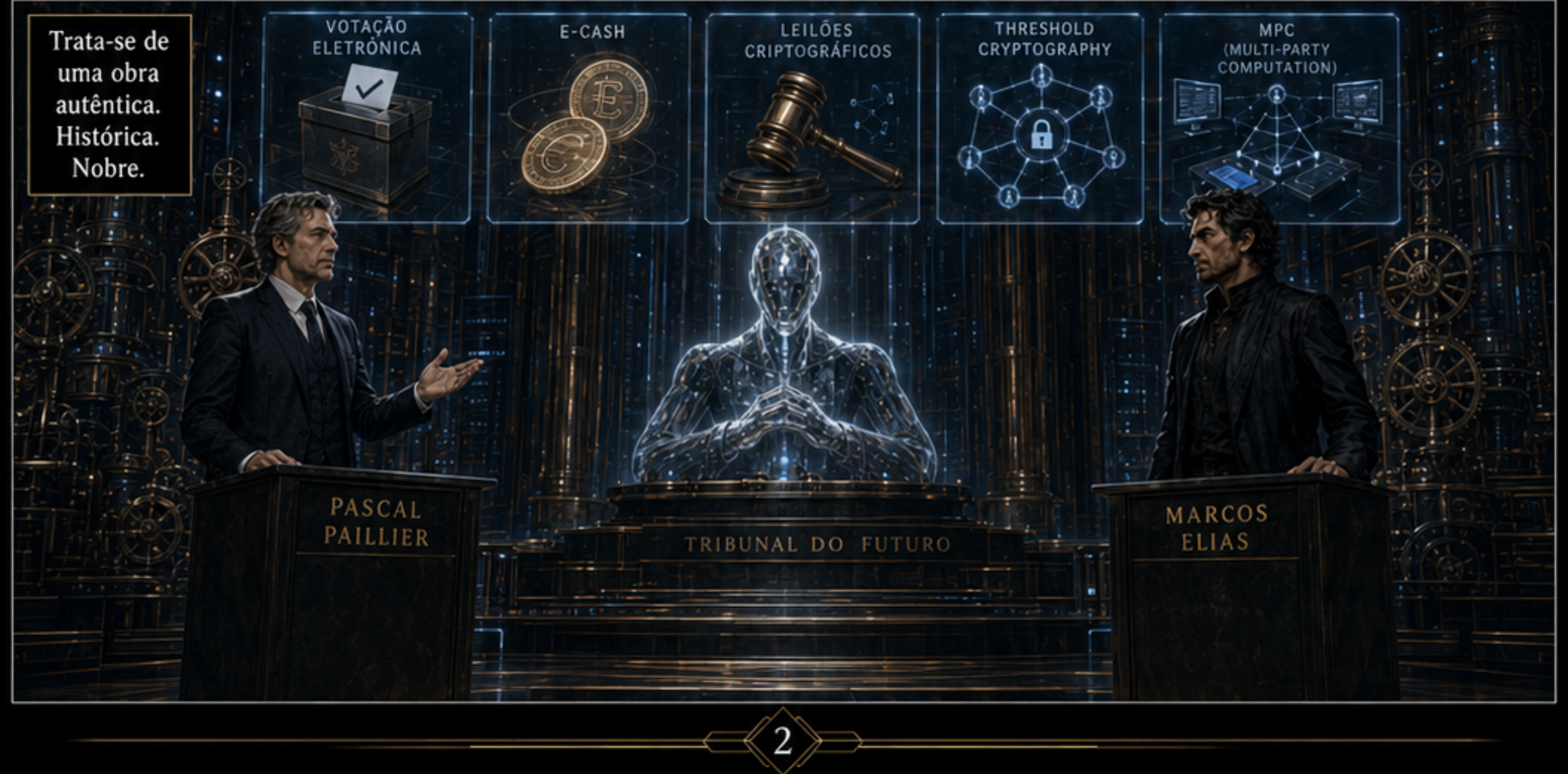
Eu dei ao mundo uma maneira elegante de somar sem expor.

$Enc(m_1 + m_2)$

$$Dec(Enc(m_1 + m_2)) = m_1 + m_2$$

RESULTADO DESCRIPTOGRAFADO

Trata-se de uma obra autêntica. Histórica. Nobre.



MOCK THETA: O TRIBUNAL DO FUTURO

Mas toda arquitetura tem seu domínio.

PAILLIER
HOMOMÓRFICO ADITIVO
SEGURO SOB DLP

PAILLIER MACHINE

- Codificação: $\mathbb{Z}_n$
- Segurança: Decisional Composite Residuosity (DCR).
- Operação: Adição homomórfica $E(m_1) \cdot E(m_2) = E(m_1 + m_2)$

Paillier preserva com clareza uma estrutura aditiva.

ESPAÇO DAS MENSAGENS
$m_1,\ m_2 \in \mathbb{Z}_n$

ESPAÇO CIFRADO
$E(m_1),\ E(m_2) \in \mathbb{Z}_{n^2}^*$

ADITIVIDADE HOMOMÓRFICA
$E(m_1) \cdot E(m_2) = E(m_1 + m_2)$

É poderosa para soma confidencial. Não é, por si só, uma gramática geral de computação confidencial.

EXPANSÃO PARA CIRCUITOS GERAIS

MULTIPLICAÇÃO
$m_1 \cdot m_2$

COMPUTAÇÃO ARBITRÁRIA

O CAMINHO SE ESTREITA.

Sua base pertence ao grande território das construções assimétricas clássicas.

CRIPTOGRAFIA ASSIMÉTRICA CLÁSSICA

- Fatoração de inteiros (RSA)
- Logaritmo discreto (Diffie-Hellman, ECC)
- Resíduo composto (Paillier)
- Suposições no modelo clássico

Segurança no modelo clássico

MÓDULOS E ESTRUTURAS
$\mathbb{Z}_n,\ \mathbb{Z}_{n^2}^*,\ \mathbb{Z}_{nn^2}^*$

n

TEOREMAS E REDUÇÕES

Segurança ⇒ DCR

Problema Difícil
↓
Redução
↓
DCR

Num mundo de computação quântica tolerante a falhas, o limite deixa de ser nota de rodapé. Torna-se destino estrutural.

Em meu tempo, isso foi extraordinário.

PASCAL PAILLIER

ERA QUÂNTICA TOLERANTE A FALHAS

- Shor: fatoração e log discreto em tempo polinomial
- Novos paradigmas criptográficos: reticulados, códigos, multivariados, isogenias, hash-based
- Segurança: informação-teórica ou pós-quântica

PARA A PAILLIER MACHINE:
LIMITE ESTRUTURAL INERENTE.

Do outro lado não está um herdeiro institucional da criptografia.

q-Pochhammer

$$(a;q)_n = \prod_{k=0}^{n=1} (1 - aq^k)$$

Jacobi Triple Product

$$\sum_{n=-\infty}^{\infty} q^{n^2} z^n = (q;q)_\infty (-z;q)_\infty (-q/z;q)_\infty$$

modular $\tau \in H$

$$q = e^{2\pi i \tau}$$

Está um estreante na criptografia formal. Mas não um espirito ordinário.

Funções Mock Theta

$$f(q) = \sum_{n=0}^{\infty} \frac{q^{n^2}}{(q;q^2)_{n+1}}$$

$$g(q) = \sum_{n=0}^{\infty} \frac{q^{n(n+1)}}{(-q;q)_n}$$

maçex bidest.

$$1 + \sum_{n=1}^{\infty} \frac{q^{n(5n-1)/2}}{(-q;q)_k^2}$$

Assintóticas

as $q \to 1^-$

$$f(q) \sim \frac{A}{(1-q)^\alpha} e^{\frac{B}{1-q}} + \sum_k C_k (1-q)^{\beta_k}$$

Topologia

- Homologia persistente
- Invariantes $\Rightarrow \mathbb{Z}$

Engenheiro, matemático, cientista da computação, modelador de risco.

ENGENHARIA

MATEMÁTICA

$\mathbb{Z}, \mathbb{N}, \mathbb{R}, \mathbb{C}$

$\int f(x)\,dx$

$\sum_{n=1}^{\infty} \frac{1}{n^6}$

$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^6}$

CIÊNCIA DA COMPUTAÇÃO

```
def ntt(a, root):
  n  = len(a)
  if n == 1: return a
  a0 = ntt(a[::2], root*root)
  a1 = ntt(a[1::2], root*root)
  w = 1
  y = [0]*n
  for k in range(n//2):
    y[k] = (a0[k] + w*a1[k]) % MOD
    y[k+n//2] = (a0[k] - w*a1[k]) % MOD
    w = (w * root) % MOD
return y
```

RISCO

SISTEMAS QUANTITATIVOS

Os estabelecidos preferem arquiteturas legiveis. O *outsider* nasce onde a legibilidade termina.

$$f(q) = \sum_{n=0}^{\infty} \frac{q^{n^2}}{(q;q^2)_{n+1}}$$

$f(q) \notin S_k(\Gamma)$

$q \to 1^-$

$\sim e^{\frac{C}{1-q}}$

γ_1 γ_2 γ_3 γ_3

π_1

Extensões não desprendíveis

$$0 \to M \to \hat{M} \to Q \to 0$$

$\delta : Q \to H^1(\Gamma, M)$

$\dim_{\mathbb{C}} M_k^!(\Gamma)$

$\neq \dim_{\mathbb{C}} S_k(\Gamma)$

Não quero melhorar uma ferramenta.

$$f(q) = \sum_{n=0}^{\infty} \frac{q^{n^2}}{(q;q^2)_{n+1}} \qquad q = e^{2\pi i \tau}$$

$q \to 1^-$

$$f(q) \sim \frac{A}{(1-q)^\alpha} e^{\frac{B}{1-q}}$$

$$\prod_{n=1}^{\infty} (1-q^n)^{24} = \Delta(\tau)$$

MOCK THETA

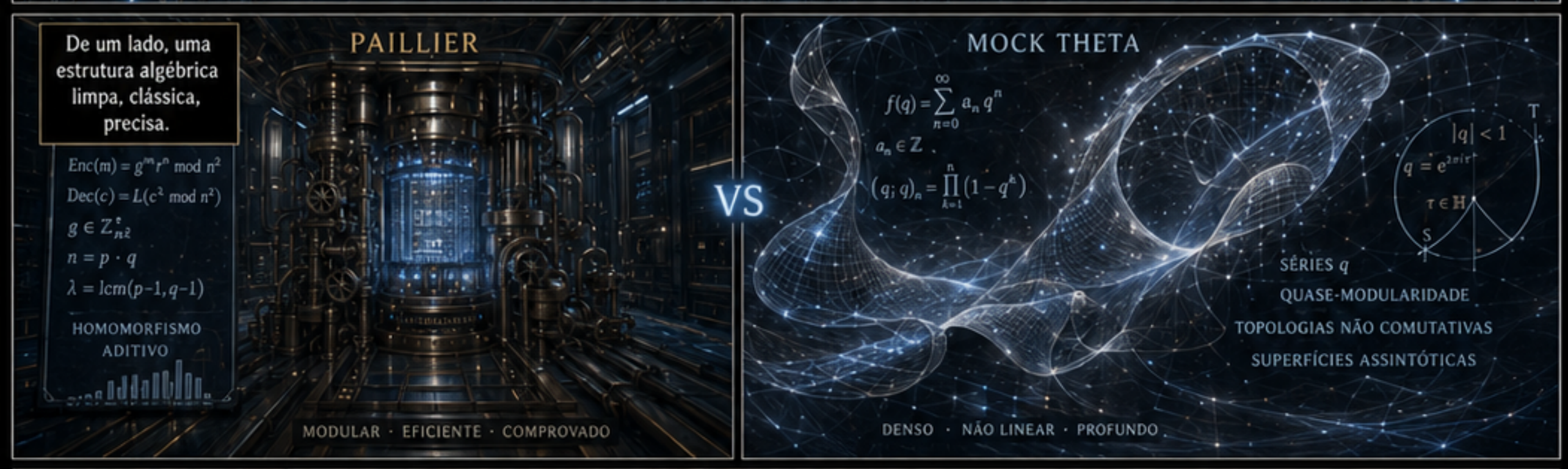
$$\left(-\frac{1}{\tau}\cdot\right) = (-i\tau)^k f(\tau) + R(\tau)$$

$$\sum_{n=-n_0}^{\infty} q^{n^2} z^n$$

Quero deslocar o eixo do problema.

Mock Theta faz a mesma coisa que Paillier?

Que arquitetura é mais adequada à era em que a criptografia precisa sobreviver ao colapso das hipóteses RSA-like e sustentar infraestrutura soberana?



A hipótese Mock Theta não se apresenta como um ajuste marginal.

MOCK THETA

SÉRIES q

$$f(q) = \sum_{n=0}^{\infty} \frac{q^{n^2}}{(-q;q)_n}$$

$$g(q) = \sum_{n=0}^{\infty} \frac{q^{n\frac{(n+1)}{2}}}{(q;q)_n}$$

$$h(q) = \sum_{n=0}^{\infty} (-1)^n \frac{q^{n(3n-\frac{1}{2})}}{(q;q)_n}$$

SUPERFÍCIES MODULARES

$\tau \in \mathbb{H}$

$q \to e^{2\pi i \tau}$

Ela procura inspiração em objetos de outra natureza.

FUNÇÕES MOCK THETA

$$f(q) = \sum_{n=0}^{\infty} \frac{q^{n^2}}{(-q;q)_n}$$

$q = e^{2\pi i \tau}$

ONDAS ASSINTÓTICAS

SIMETRIAS QUASE-MODULARES

$$f\left(\frac{a\tau+b}{c\tau+d}\right) \approx (c\tau+d)^k f(\tau) + R(\tau)$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$$

TERMO NÃO-HOLOMORFO (SOMBRA)

$\mathrm{Im}\,\tau$

$\mathrm{Re}\,\tau$

$\tau \in \mathbf{H}$

$$R(\tau) = \sum_{n=-\infty}^{\infty} r(n)\, \widehat{\Gamma}(\tau)\, q^{-n^2}$$

Não é apenas outra equação. É outro terreno.

TERRENO CLÁSSICO

Estruturas planas.
Simetrias rígidas.
Previsibilidade.

$y = ax + b$

$E : y^2 = x^3 + ax + b$

NOVO TERRENO DE MOCK THETA

Geometrias vivas.
Simetrias flexíveis.
Estruturas que respondem.

Redes modulares

Conexões não-locais

Sombras não-holomorfas

Topologias dinâmicas

A promessa está aqui: deslocar a geometria do ataque.

FERRAMENTAS CLÁSSICAS DE ATAQUE

FATORAÇÃO

LOG DISCRETO

ROTAS PADRÃO

TERRENO DE MOCK THETA

Estruturas reconfiguram.
Simetrias desviam.
Padrões se dissolvem.

$N = p \cdot q$

$g^x \equiv h \pmod{p}$

MOCK THETA

$$f(q) = \sum_{n=0}^{\infty} \frac{q^{n^2}}{(-q;q)_n}$$

SIMETRIAS QUASE-MODULARES

$$f\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^k f(\tau) + R(\tau)$$

$$R(\tau) = \sum_{n=-\infty}^{\infty} r(n)\, q^{-n^2}$$

Se a estrutura de ataque muda, a própria economia da criptoanálise muda com ela.

TRIBUNAL DO FUTURO

Não invulnerabilidade.
Não milagre.
Mas mudança de categoria.

MOCK THETA: O TRIBUNAL DO FUTURO

A cifra do século XXI não é julgada apenas pela beleza de sua construção.

PLATAFORMA GLOBAL DE ATAQUE

GPU CLUSTERS | ASIC FARMS | QUANTUM LABS

Ela é julgada pela resistência à industrialização do ataque.

ATAQUES DE TEXTO-ESCOLHIDO

Oráculos adaptativos

C → Dec() → m?

m?

WERIFICAÇÃO FORMAL

Propriedades provadas

- ☑ Corretude
- ☑ Segurança
- ☑ Invariantes
- ☑ Resistência

PROVADO

CRIPTOANÁLISE ASSISTIDA POR ML

Modelos de linguagem

Grafos de dependência

ANÁLISE DE CANAIS AUXILIARES

Power traces

EM traces

Timing

ATAQUES ADAPTATIVOS

Exploração iterativa

O inimigo não é um gênio isolado.

RECURSOS ILIMITADOS

AUTOMAÇÃO
ESCALA
PERSISTÊNCIA
COORDENAÇÃO

É uma ecologia inteira de ruptura.

MÁQUINA PAILLIER

MOCK THETA

CIFRA CLÁSSICA – PAILLIER

MÓDULO COMPOSTO $n = pq$

PADDING ESTRUTURADO

IMPLEMENTAÇÃO (CÓDIGO, TIMING)

ALEATORIEDADE $(R, r_n^n \bmod n_j^2)$

SUPERFÍCIE CONHECIDA

Na cifra clássica, o atacante sabe onde procurar.

Numa arquitetura nova, o custo inicial de modelagem adversarial pode ser maior — se a especificação for sólida.

ARQUITETURA NOVA – MOCK THETA

MODELOS PROVISÓRIOS

MOCK THETA: O TRIBUNAL DO FUTURO

1 RESISTÊNCIA PÓS-QUÂNTICA

CLÁSSICO MODULAR SOB PRESSÃO QUÂNTICA

- ⚠ Fatoração
- ⚠ Logaritmo discreto

PAISAGEM PÓS-QUÂNTICA MAIS ABERTA

- ✓ Problemas hard para computadores quânticos
- ✓ Flexibilidade para novos paradigmas

2 EXPRESSIVIDADE ESTRUTURAL

FUNCIONAL, PORÉM LIMITADA

- Adição homomórfica
- Multiplicação por escalar

RICA, MULTIDIMENSIONAL E COMPOSTA

- Operações compostas
- Camadas algébricas diversas
- Composabilidade nativa

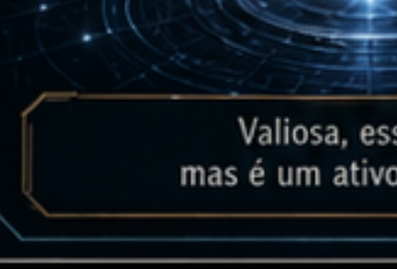
3 SUPERFÍCIE DE ATAQUE

PAILLIER: MAPA DE ATAQUES CONHECIDO

MOCK THETA: MAPA MENOS CANÔNICO

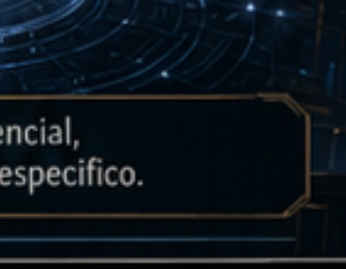
4 ADEQUAÇÃO ESTRATÉGICA

NÚVEM CONFIDENCIAL



- Computação segura
- Privacidade de dados
- Terceirização confiável

SOBERANIA DE DADOS



- Controle nacional
- Leis e jurisdições
- Independência digital

IDENTIDADE DIGITAL

- Provas de identidade
- Credenciais verificáveis
- Privacidade por design

SERVIÇOS FINANCEIROS

- KYC/AML confidencial
- Relatórios regulatórios
- Cálculos sobre dados

BLOCKCHAIN E WEB3

- Contratos inteligentes
- Privacidade on-chain
- Interoperabilidade

HARDWARE SECURITY

- Enclaves e HSMs
- Raízes de confiança
- Proteção de chaves

5 VALOR ECONÔMICO E CIVILIZACIONAL

Valiosa, essencial, mas é um ativo especifico.

Multiplicadora de possibilidades, sustenta ecossistemas e civilizações.


Tudo isso é muito belo.
GALERIAS DO TRIBUNAL
CRIPTOGRAFIA NÃO É PROMESSA. É PROVA.
REVISÃO ANTES DA ADOÇÃO
ENGENHARIA NÃO É FEITIÇARIA.
CÉTICOS POR OFÍCIO. VERIFICADORES POR MISSÃO.
DESCONFIE. MEÇA. PROVE.
Mas novidade não é segurança.
BENCHMARKS
RELATÓRIO DE AUDITORIA
AUDITORIA INDEPENDENTE
RELATÓRIO DE SEGURANÇA
Uma cifra séria nasce de definição formal, hipótese de dureza, prova, implementação, criptoanálise aberta e revisão por pares.
CRIPTOSSISTEMA PAILLIER
Criptografia Aditivamente Homomórfica
$Enc(m_1) \cdot Enc(m_2) = Enc(m_1 + m_2)$
$g^m \cdot r^n \bmod n^2$
$Dec(c) = L(c^\lambda \bmod n^2)$
Sim.
MOCK THETA
$f(q) = \sum_{i=0}^{\infty} a_i q^{e_i}$
$a_i \in Z$
$f(q) = \sum_{i=0}^{\infty} \frac{(-1)^i q^{i^2}}{(q;q^2)_i}$
$g^{i^2} \bmod n^2$
E isso não enfraquece a tese. Organiza o caminho.
Foi assim com RSA, ECC, lattices, códigos, isogenias e FHE. Nenhuma criptografia nasce madura.
TRIBUNAL DO FUTURO

Uma cifra clássica bem estabelecida é uma joia.

Paillier

Uma nova família criptográfica pode tornar-se uma infraestrutura.

BANCOS
MOCK THETA
CONFIDENCIALIDADE EM NUVEM
CUSTÓDIA DIGITAL
DATA CENTERS
IDENTIDADE DIGITAL
VOTAÇÃO ELETRÓNICA
SEGURANÇA DE HARDWARE

Se pós-quântica, eficiente, auditável é implementável...

BANCOS
EDUCAÇÃO
MOCK THETA
GOVERNO
INDÚSTRIA
SAÚDE
COMÉRCIO GLOBAL

Esta é a diferença entre ferramenta e plataforma.

TRIBUNAL DO FUTURO

Pascal Paillier: sua obra deve ser honrada.

Marcos Elias: se sua hipótese for formalizada, provada, implementada, atacada, auditada e sobreviver...

PASCAL PAILLIER

MARCOS ELIAS

...então ela não será apenas alternativa a uma cifra clássica. Será superação de categoria.

Honra-se o mestre. E então pergunta-se, sem piedade: quem protegerá os próximos trinta anos?