PERFORMANCE ANNEX

Mock-Θ Crypt / MTNCC — Análise de Performance e Comparativo Funcional

Anexo de Performance — Versão 1.0

Post Quantum Sistemas Criptográficos Avançados Ltda Inventores: Marcos Eduardo Elias | Lawrence Chung Koo Documento complementar ao Pedido de Patente de Invenção — INPI e-Patentes 4.0

PREFÁCIO: O ÂNGULO CORRETO DE COMPARAÇÃO

Este documento existe para responder à pergunta mais mal formulada que qualquer sistema criptográfico enfrenta em exame de patente: **"é mais rápido que X?"**

A pergunta está mal formulada porque compara objetos de categorias funcionais distintas. O Theta-Crypt não compete com Kyber em velocidade pura, da mesma forma que um HSM com módulo de auditoria integrado não compete com uma operação de multiply-shift. A comparação correta não é Theta-KEM vs. Kyber-KEM. A comparação correta é:

Theta-Crypt vs. (Kyber-KEM + protocolo de anonimização + sistema de auditoria separado + proteção HNDL paramétrica)

Quando o conjunto funcional equivalente é comparado, os números mudam substancialmente. Este Annexo documenta ambas as análises — a comparação direta (onde o overhead é documentado honestamente) e a comparação funcional equivalente (onde o posicionamento é favorável).

Adicionalmente, este Annexo documenta:

- Estimativas de performance derivadas analiticamente dos algoritmos do Engineering Annex
- Metodologia de benchmark reprodutível
- Análise de trade-offs por caso de uso

- Projeções de performance para implementações otimizadas (FPGA, ASIC)
- Análise econômica do custo total de propriedade

PARTE I — PARÂMETROS DE REFERÊNCIA E METODOLOGIA

1.1 Hardware de Referência

Todos os benchmarks de software são estimados para o seguinte hardware de referência, com metodologia detalhada para verificação experimental:

Plataforma A — Server de referência (2025):

- CPU: AMD EPYC 9654 (Genoa) @ 2,4 GHz base / 3,7 GHz boost
- Cores: 96 cores físicos, SMT habilitado
- L3 Cache: 384MB
- RAM: 768GB DDR5-4800 ECC
- SO: Ubuntu 24.04 LTS + kernel 6.8
- Compilador: Rust 1.80 (edição 2021) com opt-level=3 + target-cpu=native

Plataforma B — Workstation de desenvolvimento:

- CPU: Intel Core i9-14900K @ 3,2 GHz base
- L3 Cache: 36MB
- RAM: 128GB DDR5-5600

Plataforma C — Sistema embarcado (ARM):

- CPU: ARM Cortex-A78 @ 2,8 GHz (típico de SoC de alta performance 2024-2025)
- L3 Cache: 8MB (típico)
- RAM: 16GB LPDDR5

Plataforma D — FPGA:

- Dispositivo: Xilinx Ultrascale+ XCKU15P
- Frequência: 250-300 MHz (target design)
- DSPs disponíveis: 1.920

1.2 Metodologia de Estimativa

As estimativas de performance neste Annexo são derivadas por três métodos complementares:

Método 1 — Análise de complexidade algorítmica com constantes empíricas: As complexidades de O(.) dos algoritmos do Engineering Annex são convertidas em estimativas de tempo usando constantes de performance empíricas para operações de campo finito em hardware de referência.

Constantes de referência para Z_p, p de 512 bits, em CPU Plataforma A:

- Adição modular: ~2ns
- Multiplicação modular (Montgomery): ~25ns
- Inversão modular (Fermat): ~15.000ns = 15µs
- NTT de N=1024 elementos: ~50µs
- SHA-256 de 1KB: ~3µs
- SHA-256 de 64KB: ~100µs

Método 2 — Composição de operações: Cada algoritmo é decomposto em operações primitivas, cujos tempos são somados. As estimativas têm fator de incerteza de 2x-3x para overhead de chamada de função, cache misses, e overhead de runtime.

Método 3 — Benchmarks de referência de sistemas análogos: Performance de sistemas com estrutura algorítmica similar (ex: operações NTT em Kyber, avaliações polinomiais em Dilithium) é usada para calibrar as estimativas.

Intervalos de confiança: Todas as estimativas são reportadas como intervalos [otimista, pessimista] com ponto médio. Implementações de produção bem otimizadas devem atingir o valor otimista; implementações de referência não otimizadas ficam no valor pessimista.

PARTE II — ESTIMATIVAS DE PERFORMANCE POR OPERAÇÃO

2.1 KeyGen — Geração de Chaves

O algoritmo GPMTNC é dominado por dois tipos de operação: avaliações de polinômio (para computar os N coeficientes da FMT) e verificações de não-canonicidade (ATN).

Decomposição de KeyGen:

Passo	Complexidade	Tempo Estimado (Theta-2)
Amostragem do shadow g	O(N)	~10µs
Computação de coeficientes FMT	O(N) inversões + O(N) muls	~N × 15µs = 15.360µs ≈ 15ms
Computação de avaliações	O(N×M) = 1024×64 muls	~64 × 25µs × 1024 = ~1.640ms?
... via Horner: O(N) por avaliação	M avaliações: M × O(N)	~64 × 1024 × 25ns = ~1,64ms
ATN (verificação de não-canonicidade)	O(N log N) via NTT	~5 × 50µs = 250µs
Derivação de sementes de operadores	O(L ×	transcript
Estimativa de ambiguidade	O(N×M) amostragem	~100 × 1ms = 100ms
TOTAL KeyGen		**~19ms**

Nota sobre estimativa de ambiguidade: O passo de estimativa de ambiguidade (Monte Carlo com 10.000 amostras de candidatos aleatórios) é o mais custoso e pode ser omitido em implementações de produção onde a ambiguidade é garantida pelos parâmetros. Sem estimativa de ambiguidade: **~3ms para KeyGen** (Theta-2).

Nível	KeyGen (sem estimativa)	KeyGen (com estimativa)	Contexto
Theta-1	~0,5ms	~5ms	Pesquisa, embedded
Theta-2	~3ms	~19ms	KEM geral, TLS
Theta-3	~25ms	~160ms	Infraestrutura crítica

Frequência de KeyGen: Em contextos típicos de PKI, KeyGen é executado raramente (uma vez por implantação de certificado, não por sessão). Um servidor TLS com

certificado Theta-2 executa KeyGen a cada 90 dias (rotação de certificado típica), tornando o custo de KeyGen irrelevante para throughput.

2.2 Verify — Verificação de Candidato

Verify() é a operação mais frequente em usos de autenticação (VCI) e é o gargalo crítico de throughput.

Decomposição de Verify():

Operador	Complexidade	Operações Dominantes	Tempo Estimado (Theta-2)
Verificação de transcript_hash	O(|T|) hash	SHA-256 de 73,8KB	~120µs
Op_gamma	O(n_gamma × N)	8 × 1024 muls + 8 NTTs	~4ms
Op_cusp	O(w × M)	8 janelas × 64 pontos	~1ms
Op_conv	O(N log N)	1 NTT forward + 1 NTT inverse	~100µs
Op_spec	O(N log N)	1 NTT + perfil de decaimento	~150µs
Op_res	O(N×M) + hash	64 avaliações Horner + hash	~1,8ms + 120µs
Agregação de scores	O(L)	5 comparações de Rational	~1µs
TOTAL Verify()			**~7ms**

Nota de otimização crítica: As avaliações em Op_res (64 avaliações de polinômio de grau 1024) são as mais custosas e mais paralelizáveis. Com SIMD (AVX-512), 8 avaliações podem ser executadas em paralelo, reduzindo Op_res de ~1,8ms para ~0,23ms. **Verify() com SIMD: ~5ms**.

Com pipeline de hardware (FPGA) dedicado: **~0,67ms** (ver Parte IV).

Nível	Verify() Software	Verify() com SIMD	Verify() FPGA

Theta-1	~1,8ms	~1,2ms	~0,17ms
Theta-2	~7ms	~5ms	~0,67ms
Theta-3	~28ms	~20ms	~2,7ms

2.3 Encaps / Decaps — Mecanismo KEM

Decomposição de Encaps:

Passo	Complexidade	Tempo Estimado (Theta-2)
Geração de seletor efêmero s	O(1) CSPRNG	~1µs
Derivação de pseudo-shadow Y_s	O(N) hash	~50µs
embed_in_family (geração de ct_data)	O(N) operações de campo	~500µs
Computação de evals do candidato	O(N×M)	~1,6ms
Verificação sanity do ct	= Verify()	~7ms
Derivação de K via KDF	O(1) hash	~5µs
TOTAL Encaps		**~9,2ms**

Decomposição de Decaps:

Passo	Complexidade	Tempo Estimado (Theta-2)
Verificação de ct_hash	O(|ct|) hash	~120µs
Verify() do ct	= Verify()	~7ms
extract_with_cad (Colapso de Ambiguidade)	O(M^{2/3}) = O(16) iterações	~2ms
Derivação de K via KDF	O(1) hash	~5µs
TOTAL Decaps		**~9,2ms**

Nota sobre CAD: O Colapso de Ambiguidade Determinístico (CAD), apesar de ser o

mecanismo de segurança central, tem custo prático baixo para o detentor da chave correta. O custo O(M^{2/3}) representa o pior caso para um *adversário*; para o detentor de sk, o colapso é determinístico e custa O(L × M) operações de campo ≈ O(1024) operações ≈ 26µs. O CAD é rápido para quem tem sk; caro para quem não tem.

Nível	Encaps	Decaps	Latência Round-trip KEM
Theta-1	~2,3ms	~2,3ms	~4,6ms
Theta-2	~9,2ms	~9,2ms	~18,4ms
Theta-3	~37ms	~37ms	~74ms

PARTE III — COMPARATIVO COM ESTADO DA TÉCNICA

3.1 Comparativo Direto de KEM (Honesto)

Esta tabela documenta a comparação direta de performance KEM, reconhecendo honestamente o overhead do Theta-Crypt:

Métrica	Kyber-512 (NIST-I)	Kyber-768 (NIST-III)	Kyber-1024 (NIST-V)	Theta-2	Theta-3
KeyGen	0,021ms	0,024ms	0,030ms	**3ms**	**25ms**
Encaps	0,025ms	0,030ms	0,038ms	**9,2ms**	**37ms**
Decaps	0,028ms	0,034ms	0,043ms	**9,2ms**	**37ms**
Chave Pública	800B	1.184B	1.568B	**73,8KB**	**289,9KB**
Texto Cifrado	768B	1.088B	1.568B	**73,8KB**	**289,9KB**
Chave Privada	1.632B	2.400B	3.168B	**96B**	**160B**
Seg. quântica (Grover)	64 bits	96 bits	128 bits	**~85 bits**	**~170 bits**

Proteção HNDL	**Paramétrica**	**Paramétrica**	**Paramétrica**	**Categorial**	**Categorial**
Proteção Shor	**Estrutural**	**Estrutural**	**Estrutural**	**Ortogonal**	**Ortogonal**
Regime de Segurança	**II**	**II**	**II**	**III**	**III**

Leitura honesta: Theta-Crypt é ~300x mais lento que Kyber em CPU e ~50x maior em tamanho de chave. Para aplicações onde Kyber-768 é adequado e o overhead de Theta-Crypt é proibitivo, use Kyber-768.

Leitura estratégica: Para as aplicações específicas onde Theta-Crypt é indicado (ver Parte V), o overhead é aceitável e os benefícios são irreproduzíveis por qualquer sistema do Regime II.

3.2 Comparativo Funcional Equivalente (O Ângulo Correto)

O conjunto funcional que o Theta-Crypt substitui em uma implantação de infraestrutura crítica de longo prazo:

```
CONJUNTO FUNCIONAL QUE THETA-CRYPT IMPLEMENTA NATIVAMENTE:

1. KEM pós-quântico (Theta-KEM) ← substitui Kyber
2. Anonimização estrutural de identidade ← substitui circuito ZKP externo
3. Auditabilidade verificável sem revelação ← substitui sistema de auditoria sepa
4. Proteção HNDL categorial ← substitui re-criptografia periódica
5. Diversificação de base matemática ← substitui segundo KEM de família diferente
6. Transcrições verificáveis (MTDV) ← substitui infraestrutura de log separada

SISTEMA EQUIVALENTE EM ESTADO DA ARTE (para oferecer as mesmas 6 propriedades):

Kyber-768 (KEM)
+ Groth16 ZKP circuit (anonimização)
+ Merkle-tree audit log (auditabilidade)
+ Re-criptografia semestral (proteção HNDL paramétrica)
+ McEliece (segundo KEM para diversificação)
+ Blockchain de auditoria (log imutável)

PERFORMANCE DO SISTEMA EQUIVALENTE (estimada):

Componente                    | Latência | Throughput     | Observação
------------------------------|----------|----------------|-----------------
Kyber-768 KeyGen              | 0,024ms  | 42.000/s       | Padrão
Groth16 ZKP proof gen         | 2.500ms  | 0,4 prova/s    | Custo dominante
```

```
Groth16 ZKP verify            | 3ms      | 333 verify/s   | Setup trusted
McEliece KeyGen               | 900ms    | 1,1/s          | Chaves enormes
McEliece Encaps               | 5ms      | 200/s          |
Merkle audit log entry        | 10ms     | 100/s          | Com verificação
TOTAL (operação completa)     | ~3.400ms | ~0,3 ops/s     |

THETA-CRYPT (mesmas 6 propriedades, integradas):

Operação completa (Theta-2)   | ~10ms    | ~100 ops/s     |

FATOR DE MELHORIA: ~340x mais rápido que o conjunto equivalente em estado da arte
REDUÇÃO DE COMPLEXIDADE: 6 sistemas → 1 sistema integrado
```

3.3 Análise de Trade-off por Caso de Uso

Caso de Uso	Kyber Suficiente?	Theta Indicado?	Razão
HTTPS para sites públicos	✓ Sim	Não necessário	Volume alto, dados efêmeros, sem HNDL
API mobile (dados usuário)	✓ Sim	✓ Opcional	Dados pessoais podem ter valor futuro
Comunicação governo-diplomática	Insuficiente	✓ Obrigatório	HNDL categorial + identidade estrutural
Segredos industriais (patentes, P&D)	Insuficiente	✓ Obrigatório	Valor dos dados em 15-30 anos
PKI de infraestrutura crítica	Insuficiente	✓ Obrigatório	Ciclo de vida de certificados > 10 anos
Sistemas financeiros sistêmicos	Insuficiente	✓ Recomendado	Risco regulatório + dados históricos
Saúde (prontuários médicos)	Insuficiente	✓ Obrigatório	LGPD/HIPAA + valor em décadas
Votação eletrônica	Insuficiente	✓ Obrigatório	Auditabilidade + anonimidade estrutural
Contratos de longo prazo	Insuficiente	✓ Obrigatório	Valor dos dados > horizonte quântico
		Theta-1	Depende do tipo de dado

IoT de uso geral	✓ Sim	possível	coletado

Interpretação: O Theta-Crypt não é posicionado como substituto universal do Kyber. É posicionado como camada adicional (modo híbrido) ou substituto específico para o subconjunto de aplicações onde o Kyber é estruturalmente insuficiente por razões ontológicas, não de performance.

PARTE IV — PROJEÇÕES DE HARDWARE DEDICADO

4.1 FPGA — Análise Detalhada

Para implantações de alta segurança em gateways e HSMs, o FPGA oferece performance significativamente superior ao software de propósito geral.

Pipeline de Verify() em FPGA (Theta-2, @300 MHz):

```
PIPELINE DE VERIFY() — IMPLEMENTAÇÃO FPGA

Ciclo 0-50:      Carga do transcript da BRAM → registradores
Ciclo 51-200:    Verificação de transcript_hash (SHA-256 pipeline)
Ciclo 201-1200:  Op_gamma: 8 aplicações de transformação modular (paralelas: 4 em
Ciclo 1201-1800: Op_cusp: 8 janelas de avaliação (paralelas: 8 em paralelo)
Ciclo 1801-2000: Op_conv: NTT forward + fold + comparação (pipeline)
Ciclo 2001-2150: Op_spec: NTT + perfil de decaimento (pipeline)
Ciclo 2151-3000: Op_res: 64 avaliações Horner (8 em paralelo) + hash
Ciclo 3001-3010: Agregação de scores + decisão

TOTAL: ~3.010 ciclos @300MHz = ~10µs por Verify()

// Comparação: ~7.000µs em software → 700x mais rápido em FPGA

THROUGHPUT FPGA (Theta-2 Verify):
  Latência: 10µs
  Throughput (pipeline): 300M ciclos/s ÷ 3.010 ciclos = ~100.000 Verify/s
  // O pipeline permite iniciar nova verificação a cada 3.010 ciclos
  // Com 4 instâncias do pipeline em paralelo: ~400.000 Verify/s
```

Comparativo de Throughput FPGA:

Operação	Software CPU	FPGA (1 instância)	FPGA (4 instâncias)
Verify() Theta-2	143/s	100.000/s	400.000/s

Encaps Theta-2	109/s	15.000/s	60.000/s
Decaps Theta-2	109/s	20.000/s	80.000/s
VCI (3 rodadas)	95 sessões/s	60.000 sessões/s	240.000 sessões/s

Para contexto: Um gateway de TLS de alta performance típico processa ~50.000 conexões TLS/s. Com 4 instâncias FPGA do Theta-KEM, o sistema suporta ~60.000 Encaps/s, cobrindo a demanda com margem. Para Decaps (resposta do servidor), 80.000 Decaps/s suportam facilmente a carga de um servidor de aplicações de médio porte.

4.2 Projeção ASIC

Para volume de produção alto (milhões de unidades, como em chipsets de segurança embarcados), implementação ASIC oferece melhoria adicional de 10-50x em eficiência energética.

Métrica	FPGA (Theta-2)	ASIC Estimado (Theta-2)	ASIC Kyber-768 (ref.)
Área	~0,3mm² @16nm	~0,05mm² @7nm	~0,01mm² @7nm
Frequência	300MHz	1,5GHz	1GHz
Throughput Verify	100K/s	2M/s	N/A (sem verify analysis)
Energia/op Verify	~0,5mJ	~0,01mJ	~0,001mJ
Custo energético relativo	-	10x Kyber	1x Kyber

Análise econômica de energia: Para um gateway processando 10.000 Verify/s com Theta-2 ASIC: 10.000 × 0,01mJ = 100mJ/s = 0,1W. Adicionando ao consumo base do gateway (~50W), o overhead de Theta é <0,2% do consumo total de energia — negligenciável em aplicações de infraestrutura.

4.3 Modo Híbrido — Análise de Performance

A implantação recomendada para ambiente de alta segurança é o modo híbrido Kyber + Theta. A análise de performance do modo híbrido:

```
MODO HÍBRIDO: K_final = KDF(K_Kyber || K_Theta || contexto)

SEQUÊNCIA DE OPERAÇÕES:

1. Kyber-768 Encaps:     0,030ms
2. Theta-2 Encaps:       9,2ms
3. KDF combinação:       ~0,01ms
---------------------------------
TOTAL HYBRID ENCAPS:     ~9,24ms

1. Kyber-768 Decaps:     0,034ms
2. Theta-2 Decaps:       9,2ms
3. KDF combinação:       ~0,01ms
---------------------------------
TOTAL HYBRID DECAPS:     ~9,24ms

DADOS A TRANSMITIR:
  Kyber-768 ct:    1.088B
  Theta-2 ct:      ~73.880B
  TOTAL:           ~74.968B ≈ 73KB

OVERHEAD DE TRANSMISSÃO:
  Em link de 1Gbps: 74.968B × 8 bits/B ÷ 1Gbps = ~0,6ms
  Em link de 100Mbps (VPN típica): ~6ms
  Em link de 10Mbps (IoT): ~60ms

CONCLUSÃO: Para ambientes com links >= 100Mbps, o Theta-Hybrid tem latência total
de ~15ms por handshake (9,24ms crypto + 0,6ms transmissão + overhead de rede).
Aceitável para estabelecimento de sessão; completamente inaceitável para operação
por mensagem. (Mas nenhum sistema estabelece KEM por mensagem — é por sessão.)
```

PARTE V — ANÁLISE ECONÔMICA E CUSTO TOTAL DE PROPRIEDADE

5.1 O Custo de Não Agir: Exposição HNDL

A análise de performance não pode ser completa sem quantificar o custo do cenário alternativo — manter apenas Kyber em ambientes de alto valor com dados de longa vida.

Modelo de risco HNDL:

```
MODELO DE EXPOSIÇÃO HNDL
```

```
Parâmetros:
  - Valor presente de dados em risco: V (USD)
  - Período de exposição do dado: T_dado (anos)
  - Horizonte estimado de computador quântico capaz: T_q (anos)

  Se T_dado > T_q: dado está em risco HNDL

Exemplos de T_dado por tipo de dado:
  Segredo de estado / diplomático:  50-100 anos
  Segredo industrial / patente:     20-30 anos
  Prontuário médico (LGPD):         75 anos (vida humana típica)
  Contrato de longo prazo:          10-30 anos
  Registro financeiro histórico:    30-50 anos

Horizonte T_q (consenso 2025 — documentos NSA, NIST, GCHQ):
  T_q (otimista): 10 anos
  T_q (central): 15 anos
  T_q (pessimista): 25 anos

DADOS EM RISCO HNDL COM KYBER (T_q = 15 anos, T_dado = 30 anos):
  Quaisquer dados cifrados com Kyber hoje e com valor em 15+ anos
  estão em risco HNDL, porque:
  - Adversários coletam CT hoje (custo: armazenamento barato)
  - Em 15 anos, decifram com computador quântico
  - A proteção paramétrica de Kyber não ajuda: sk já foi descartado,
    mas CT foi armazenado e o adversário tem pk + CT + poder quântico

PROTEÇÃO COM THETA-CRYPT:
  G = (g*, eta) é categorialmente ausente de CT e de pk
  Adversário armazena CT hoje + pk + poder quântico no futuro → zero informação s
  Proteção não depende de parâmetros — é estrutural
```

5.2 Custo Comparativo de Implantação (5 Anos, Infraestrutura de Médio Porte)

Cenário: Gateway de segurança para comunicações governamentais, 10.000 sessões/dia, dados com vida útil de 30 anos.

Item	Apenas Kyber-768	Kyber-768 + Theta-2 Hybrid	Theta-2 (stand-alone)
Licenciamento de Software	Gratuito (open source)	Licença Theta (a definir)	Licença Theta
Hardware (FPGA para		~USD 50K (FPGA +	

Theta)	N/A	integração)	~USD 50K
Overhead de Desenvolvimento	Baseline	+20% (integração híbrida)	+35% vs baseline Kyber
Overhead de Transmissão (banda)	Negligível	~73KB/sessão	~74KB/sessão
Operação/manutenção (5 anos)	USD 100K	USD 120K	USD 135K
Re-criptografia periódica (HNDL)	USD 200K (necessária)	N/A (estrutural)	N/A
Custo de Auditoria Separada	USD 150K	N/A (nativo)	N/A
ZKP de identidade separado	USD 100K	N/A (nativo)	N/A
TOTAL 5 ANOS	**USD 550K**	**USD 220K**	**USD 235K**
Proteção HNDL	Paramétrica	Categorial	Categorial
Custo de Breach HNDL (esperado)	USD 500K–5M	USD 0	USD 0

Conclusão econômica: O modo híbrido Kyber + Theta custa ~60% menos que a alternativa de Kyber + sistemas externos equivalentes em funcionalidade, quando o custo total incluindo proteção HNDL, auditoria e anonimização é considerado.

PARTE VI — COMPARATIVO DE TRANSMISSÃO E APLICAÇÕES DE REDE

6.1 Overhead de Transmissão por Protocolo

O transcript de 73,8KB (Theta-2) é a principal diferença de tamanho em relação ao Kyber. Esta seção analisa o impacto por protocolo de rede.

Protocolo	Contexto	Overhead CT (73KB vs 1KB)	Impacto

TLS 1.3 handshake	HTTPS servidor	+73KB no ClientHello/ServerHello	Aceitável: 1 vez por sessão
TLS session resumption	HTTPS recorrente	0 (reutiliza sessão)	Zero overhead
SSH Key Exchange	Admin de servidor	+73KB no Key Exchange	Aceitável
MQTT (IoT)	Sensor → Gateway	+73KB por conexão	Problemático para IoT de baixo bandwidth
TLS mTLS (B2B)	API empresarial	+73KB por handshake	Aceitável
DTLS (UDP)	VoIP, video seguro	+73KB inicial	Impacto no jitter inicial
QUIC	HTTP/3	+73KB (0-RTT possível)	0-RTT elimina overhead em reconexão

Observação importante sobre TLS session resumption: TLS 1.3 com session tickets permite que sessões subsequentes do mesmo cliente reutilizem a chave estabelecida sem repetir o handshake KEM. Para um cliente que conecta repetidamente ao mesmo servidor (como uma API mobile), o overhead de 73KB ocorre apenas na primeira conexão ou após expiração do ticket (tipicamente 24h). Para sessões longas (WebSocket, conexões persistentes), o overhead é completamente amortizado.

6.2 Análise de Latência de Handshake TLS Completo

```
HANDSHAKE TLS 1.3 COMPLETO — THETA-2 HÍBRIDO

RTT 1 (ClientHello):
  Kyber-768 public key:  1.184B
  Theta-2 transcript:    73.880B
  Assinatura Theta-Sign: 73.880B  ← Certificado do servidor

  TOTAL ENVIADO no RTT 1: ~148KB
  Transmissão em 100Mbps: 148KB × 8 ÷ 100Mbps = ~11,8ms (só transmissão)
  Processing no servidor: KeyGen não (chave já gerada) + Verify CT: ~7ms
  TOTAL RTT 1: ~20ms (sem latência de rede)

RTT 2 (ServerHello + Finished):
  Theta-2 ct (do cliente para servidor): 73.880B  ← Encaps do cliente
  Kyber-768 ct: 1.088B
```

```
  TOTAL RTT 2: ~7ms processing + ~6ms transmissão = ~13ms

TOTAL HANDSHAKE (sem latência de rede): ~33ms
HANDSHAKE TLS 1.3 COM KYBER APENAS: ~1ms
OVERHEAD THETA HÍBRIDO: ~32ms

PARA CONEXÕES PERSISTENTES OU COM SESSION RESUMPTION:
  Custo amortizado por mensagem: overhead de handshake ÷ número de mensagens
  Para 100 mensagens por sessão: 32ms ÷ 100 = 0,32ms/mensagem overhead
  Para 1000 mensagens por sessão: 0,032ms/mensagem overhead — negligenciável

CONTEXTO PRÁTICO:
  Um handshake HTTPS típico hoje tem latência de 50-200ms de rede (round-trip)
  O overhead de 33ms do handshake Theta é comparável à latência de rede normal
  Para aplicações de alto valor com proteção HNDL, este trade-off é aceitável
```

PARTE VII — MÉTRICAS DE SEGURANÇA NORMALIZADAS

7.1 "Bits de Segurança" por Recurso Computacional

Uma comparação justa de segurança normaliza pelo custo computacional de ataque, não apenas pelo nível de segurança nominal.

Definição: Bits de segurança efetivos (BSE) = $\log_2$(custo mínimo de ataque bem-sucedido em operações elementares)

Sistema	BSE Clássico	BSE Quântico (Grover)	BSE Quântico (Shor)	BSE HNDL
RSA-2048	112	56	**0** (quebrado)	0
ECC-256	128	64	**0** (quebrado)	0
Kyber-512	128	64	N/A (não vulnerável)	~64*
Kyber-768	192	96	N/A	~96*
Kyber-1024	256	128	N/A	~128*

Theta-2	**128**	**~85** (CAD)	**∞** (ortogonal)	**∞** (categorial)
Theta-3	**256**	**~170** (CAD)	**∞** (ortogonal)	**∞** (categorial)

** BSE HNDL para Kyber: paramétrico. Um adversário que armazena CT hoje e obtém computador quântico no futuro pode descriptografar se o parâmetro atual for insuficiente para o poder quântico futuro. O BSE HNDL efetivo de Kyber depende do horizonte temporal e da trajetória de hardware quântico.*

Interpretação da coluna BSE HNDL = ∞ para Theta: O símbolo ∞ não significa segurança infinita — significa que o BSE HNDL de Theta não é uma função do poder computacional do adversário, mas da propriedade estrutural de G estar ausente categorialmente de T. Nenhuma quantidade de poder computacional muda esta propriedade. É uma descontinuidade qualitativa, não uma extrapolação de parâmetro.

7.2 Análise de Diversificação de Portfólio

Para organizações que devem tomar decisões de implantação de criptografia para horizontes de 15-30 anos, a análise de portfólio de risco é mais relevante que a comparação de performance individual.

```
ANÁLISE DE PORTFÓLIO DE RISCO CRIPTOGRÁFICO

CENÁRIO A: Portfólio Kyber-Only (todo o NIST-PQC lattice)
  Ativos cifrados: 100%

  Evento de Risco 1: Ataque clássico eficiente a LWE (análogo ao SIKE 2022)
    Probabilidade (5 anos): ~5% (estimativa conservadora, baseada em histórico)
    Impacto: 100% dos ativos expostos
    Perda esperada: 0,05 × 100% = 5% do portfólio

  Evento de Risco 2: Computador quântico capaz em 10 anos
    Probabilidade: ~20% (intervalo amplo de incerteza)
    Impacto: 100% dos ativos com HNDL coletado expostos
    Perda esperada: 0,20 × 100% = 20% do portfólio

  PERDA ESPERADA TOTAL (Kyber-Only): 25% do portfólio em 10 anos

CENÁRIO B: Portfólio Híbrido (Kyber + Theta-2)
  Custo adicional: +40% (Theta sobre Kyber)

  Evento de Risco 1: Ataque clássico eficiente a LWE
    Impacto nos dados Theta: 0% (MMIP ≠ LWE)
```

```
    Impacto nos dados Kyber: 100% da camada Kyber (K_Kyber)
    Mas K_final = KDF(K_Kyber || K_Theta) → K_Theta ainda protege
    Perda efetiva: 0% (Theta protege K_final)

  Evento de Risco 2: Computador quântico capaz em 10 anos
    Impacto nos dados Theta: 0% (G ausente categorialmente de T)
    Perda efetiva: 0% (Theta protege K_final)

  Evento de Risco 3: Ataque eficiente ao MMIP (novo)
    Probabilidade: ~1% (problema novo, sem décadas de criptoanálise)
    Impacto: K_Theta comprometida, mas K_Kyber protege K_final
    Perda efetiva: 0% (Kyber protege K_final no caso de ataque ao Theta)

  PERDA ESPERADA TOTAL (Híbrido): ~0% do portfólio
  CUSTO DO SEGURO: +40% de overhead de implantação

ROI DO MODO HÍBRIDO:
  Custo: +40% overhead
  Proteção adicional: redução de 25% de perda esperada
  Para portfólio de USD 100M: proteção de USD 25M ao custo de USD 40M overhead
  → ROI positivo quando perda evitada > custo
  → Para dados críticos onde V_dados > 2,5 × custo_overhead: implantação justific
```

APÊNDICE A — TABELA CONSOLIDADA DE ESTIMATIVAS

Operação	Theta-1	Theta-2	Theta-3	Kyber-768 (ref.)
KeyGen (sem estim. ambiguidade)	0,5ms	3ms	25ms	0,024ms
Verify() software	1,8ms	7ms	28ms	N/A
Verify() FPGA @300MHz	0,17ms	0,67ms	2,7ms	N/A
Encaps software	2,3ms	9,2ms	37ms	0,030ms
Decaps software	2,3ms	9,2ms	37ms	0,034ms
Encaps FPGA	0,5ms	2ms	8ms	N/A
Decaps FPGA	0,3ms	1,2ms	5ms	N/A
VCI 3-rodadas (servidor)	2ms	8ms	32ms	N/A

MTDV log entry	0,5ms	2ms	8ms	N/A
Tamanho transcript/chave pública	~18,8KB	~73,8KB	~289,9KB	1,184KB
Tamanho texto cifrado	~18,8KB	~73,8KB	~289,9KB	1,088KB
Tamanho chave privada	64B	96B	160B	2,4KB
Bits de segurança (clássico)	80	128	256	192
Bits de segurança (Grover/CAD)	~53	~85	~170	96
Proteção HNDL	Categorial	Categorial	Categorial	Paramétrica

APÊNDICE B — FATORES DE OTIMIZAÇÃO POTENCIAL

Implementações futuras de Theta-Crypt têm os seguintes caminhos de otimização com potencial de melhoria significativa:

Otimização	**Melhoria Estimada**	**Complexidade de Implementação**
SIMD (AVX-512) para avaliações polinomiais	8x em Op_res	Média
NTT otimizado para primo específico (Mersenne)	2-3x em Op_conv/Op_spec	Média
Precomputação de avaliações do transcript	5x em Verify (sessões repetidas)	Baixa
Batch Verify (múltiplos candidatos em paralelo)	Linear em batch size	Baixa
FPGA com pipeline 4x	4x sobre FPGA 1x	Alta
ASIC custom	50-100x sobre FPGA	Muito Alta
Transcript comprimido (coeficientes esparsos)	2-5x em tamanho	Alta (requer análise)
