Expansão Teórica 40 — Criptografia, Coerência Computacional e a Segurança por Dissociação Vetorial

Resumo

Nesta expansão, é apresentado o fundamento estrutural da segurança criptográfica a partir da Teoria ERIЯ∃ e da Teoria das Singularidades Ressonantes (TSR). Demonstramos que sistemas como o RSA operam intencionalmente com **projeções coerentes de resolução (criptografia)** e **dissociações vetoriais na reversão (fatoração)**. A separação entre os domínios helicoidal $\mathbb{D}_H$ e toroidal $\mathbb{D}_T$ garante a assimetria computacional entre encriptação e quebra, sendo esta última associada à classe NP. Assim, a conjectura P ≠ NP fundamenta diretamente a segurança desses sistemas, que exploram a **quebra da coerência vetorial na projeção inversa**.

1. Fundamento Criptográfico Tradicional

O sistema RSA baseia-se em duas premissas:

- A operação direta (criptografia) é fácil:

$$\mathcal{E}_{RSA}(m) = c = m^e \mod N$$

- A operação inversa (fatorar $N = p \cdot q$) é difícil sem a chave privada.

A dificuldade está no fato de que, dado N, encontrar (p, q) exige **fatoração**, um problema pertencente à classe **NP**, mas presumivelmente **não em P**.

2. Estrutura Computacional na TDC

O espaço computacional geral é estendido como:

$$\mathcal{C} = \mathbb{D}_E \oplus \mathbb{D}_T \oplus \mathbb{D}_H$$

onde:

- $\mathbb{D}_E$: Domínio Esférico — ordem e estabilidade;
- $\mathbb{D}_T$: Domínio Toroidal — ciclos não determinísticos;
- $\mathbb{D}_H$: Domínio Helicoidal — projeções vetoriais coerentes.

A criptografia opera entre esses domínios, utilizando **projeções coerentes para encriptação** e forçando o atacante a buscar **reversão por trajetórias toroidais incoerentes**.

3. Dissociação de Coerência como Base da Segurança

Definimos:

- $\mathcal{E}(x)$: operação EIRE (criptografia direta);
- $\mathcal{R}(y)$: operação RIRE (verificação ou tentativa de quebra);
- $\tau(x)$: projeção vetorial coerente helicoidal da entrada.

Um sistema criptográfico é seguro se:

$$\boxed{\mathcal{E}(x) \in \mathbb{D}_H \quad \wedge \quad \mathcal{E}^{-1}(x) \notin \mathbb{D}_H}$$

Ou seja, **a encriptação é uma projeção coerente**, mas **a reversão não é** — está fora do domínio vetorial.

4. Fatoração como Trajetória Toroidal

A tentativa de reverter $N = p \cdot q$ pode ser escrita como:

$$\mathcal{E}^{-1}(N) = \sum_{n=1}^{N} \mathcal{R}(y_n), \quad y_n \in \mathbb{D}_T$$

A coerência só é atingida para algum $y_{n_0} = (p, q)$, mas não existe trajetória vetorial direta para isso.

$$(p, q) \notin \mathbb{D}_H \quad \Rightarrow \quad \text{resolução via busca não vetorial (NP)}$$

5. Condição Estrutural de Segurança Criptográfica

Dado um sistema criptográfico Σ, definimos:

$$\Sigma = \{\mathcal{E}, \mathcal{D}, \mathcal{K}_{\text{pub}}, \mathcal{K}_{\text{priv}}\}$$

É seguro se a operação inversa não reside no plano helicoidal:

$$\boxed{\mathcal{E}^{-1} \notin \mathbb{D}_H}$$

Esta é a **expressão geométrica da dissociação vetorial intencional** que garante a segurança do sistema.

6. Criptografia Quântica e a Expansão Coerencial

Algoritmos como o de Shor realizam fatoração eficiente utilizando **superposição quântica**. No formalismo TDC, isso equivale a operar em um domínio estendido:

$$\mathbb{D}_Q = \text{Domínio de Projeções Superpostas}$$

$$\mathbb{D}_{H+Q} = \mathbb{D}_H \oplus \mathbb{D}_Q$$

A reversão da criptografia clássica só é possível porque $\mathcal{E}^{-1} \in \mathbb{D}_{H+Q}$, **expandindo artificialmente a coerência vetorial**.

Isso reforça a necessidade de novas formas de criptografia baseadas em domínios não vetoriais nem quantizáveis.

7. Conclusão

A segurança de sistemas criptográficos como o RSA decorre da **dissociação vetorial entre encriptação e decriptação**. O operador direto está em $\mathbb{D}_H$, mas sua inversa está fora dele, exigindo exploração no domínio toroidal (NP).

$$\boxed{\text{RSA é seguro} \iff \mathcal{E} \in \mathbb{D}_H \quad \wedge \quad \mathcal{E}^{-1} \in \mathbb{D}_T \setminus \mathbb{D}_H}$$

A Teoria ERIЯƎ oferece uma estrutura formal e geométrica para modelar, avaliar e construir criptografias que se sustentem sobre **coerência vetorial parcial** e **projeções assimétricas**, mantendo a segurança contra reversões por colapso de coerência.