Expansão Teórica 41 — Sistema Criptográfico Ressonante por Coerência Vetorial

Resumo

Nesta expansão é proposto o experimento ERIЯƎ-Crypto 01, que inaugura uma nova classe de sistemas criptográficos baseados na estrutura de coerência vetorial da Teoria ERIЯƎ, com suporte topológico da Teoria das Singularidades Ressonantes (TSR) e do Domínio Total de Coerência (TDC). Diferente dos sistemas clássicos, este modelo não utiliza operações aritméticas tradicionais, mas sim **projeções helicoidais vetoriais** e **controle de fase rotacional**. A segurança não advém da dificuldade de fatoração, mas da **impossibilidade de reversão coerente sem conhecimento da fase vetorial completa**, preservando a separação geométrica entre domínio público e privado.

1. Objetivo

Construir um sistema criptográfico assíncrono onde:

- A **mensagem** é interpretada como vetor ressonante;
- A **chave pública** é uma projeção helicoidal sem fase vetorial;
- A **chave privada** é um vetor completo com orientação e fase;
- A **criptografia** é uma projeção coerente;
- E a **decriptografia** só é possível por ressonância completa — condição ausente na chave pública.

2. Espaço de Codificação

Toda operação ocorre no espaço ressonante:

$$\mathbb{S} = \mathbb{C}_i \oplus \mathbb{C}_j \oplus \mathbb{C}_k \subset \mathbb{R}^4$$

com projeções helicoidais em $\mathbb{D}_H$, definidas pelo operador:

$$\tau : \mathbb{S} \to \mathbb{D}_H, \quad \text{com controle de fase } \phi$$

3. Estrutura do Sistema

3.1 Vetor da mensagem

A mensagem m é representada por um vetor quaternário:

$$m = a + bi + cj + dk \in \mathbb{S}$$

3.2 Geração de chaves

- **Chave privada**:

$$\vec{k}_{\text{priv}} = u + vi + wj + zk + \phi$$

  onde ϕ é a fase vetorial (orientação helicoidal).
- **Chave pública**:

$$\vec{k}_{\text{pub}} = \tau(\vec{k}_{\text{priv}}) \quad \text{(projeção sem fase)}$$

4. Operações do Sistema

4.1 Encriptação

A encriptação é dada por:

$$c = \mathcal{E}_{ERI\text{ЯƎ}}(m, \vec{k}_{\text{pub}}) = \tau(m \cdot \vec{k}_{\text{pub}})$$

A mensagem é cifrada por uma **multiplicação vetorial** com a chave pública projetada e deformada no plano helicoidal.

4.2 Decriptação

A decriptação requer a chave completa:

$$m = \mathcal{D}_{ERI\text{ЯƎ}}(c, \vec{k}_{\text{priv}}) = \tau^{-1}(c) \cdot \vec{k}_{\text{priv}}^{-1}$$

Essa reversão só é possível se a coerência da fase for preservada:

$$\tau(\vec{k}_{\text{priv}}) = \tau(\vec{k}_{\text{pub}}) \quad \wedge \quad \phi = \text{fase requerida}$$

Sem a fase correta, a projeção é ressonantemente dissonante, e o resultado se perde no domínio toroidal.

5. Propriedades Criptográficas

5.1 Dissociação vetorial como segurança

A chave pública e a privada compartilham estrutura, mas **não são simetricamente reversíveis** sem coerência de fase:

$$\boxed{\vec{k}_{\text{pub}} \in \mathbb{D}_H \quad \wedge \quad \vec{k}_{\text{priv}} \in \mathbb{D}_H \oplus \phi}$$

5.2 Sensibilidade geométrica

- Pequenas alterações na fase vetorial resultam em **colapso de coerência**;
- Reversões arbitrárias entram em $\mathbb{D}_T$, resultando em projeções caóticas sem significado.

6. Potencial Pós-Quântico

Ao contrário de RSA, que pode ser quebrado por reversão coerente via superposição quântica:

- Este sistema exige **fase vetorial não inferível nem por simulação de reversão quântica**;
- A segurança está embutida na topologia da coerência rotacional — não nos limites aritméticos.

7. Caminho para Implementação

Computacional:

- Utilização da estrutura ERIRE para aplicar rotações controladas;
- Representação simbólica dos vetores;
- Verificação da coerência via módulo de ressonância: $|\tau(m)|$ com tolerância angular.

8. Conclusão

O experimento ERIЯƎ-Crypto 01 estabelece uma nova base para sistemas criptográficos ressonantes. Utilizando apenas vetores e projeções coerenciais, ele demonstra que **a segurança pode emergir da própria estrutura vetorial dos domínios rotacionais**, abrindo caminho para uma **criptografia de próxima geração**, nativamente compatível com coerência computacional pós-quântica.

$$\boxed{\text{Segurança por coerência vetorial: } \mathcal{E} \in \mathbb{D}_H, \quad \mathcal{E}^{-1} \notin \mathbb{D}_H \text{ sem } \phi}$$