



Hardening Criptográfico: NOCTURNE-ALETHEIA v1.1

Para atingir o **Congelamento Semântico ZK**, este documento formaliza as restrições necessárias para colmatar as lacunas entre a camada de aplicação e a camada de prova.

1. Invariantes de Domínio e Range Proofs

Diferente do Rust, onde tipos como `f64` gerem limites, no circuito ZK trabalhamos em **Campos Finitos (Scalar Field)**. O risco de *wrap-around* silencioso é real.

ZK-INV-E5: Domínio Energético (Fix)

Para evitar que `energy_efficiency` negativo subverta o multiplicador:

- **Constraint:** $E_{\text{scaled}} + 1000 \geq 0$
- **Implementação:** Componente `GreaterEqThan(n_bits)` comparando o input com o valor zero antes da atribuição ao sinal de bônus.
- **Ameaça Mitigada:** Impede que um "investigador" use um desastre energético massivo para inverter o sinal da prova e gerar reputação positiva artificialmente.

ZK-INV-E3: Validação de Incerteza (Range)

- **Constraint:** $1 \leq P, Q \leq 1.000.000$ (Assumindo precisão de 6 casas decimais).
- **Implementação:** `Num2Bits` seguido de verificação de limite superior para evitar overflow do campo primo durante o cálculo do logaritmo.

2. Especificação Formal do Logaritmo (Approximation Layer)

O cálculo de $\Delta H = \log_2(P) - \log_2(Q)$ em ZK não pode ser exato.

- **Método Escolhido:** Polinómio de Taylor de 4ª ordem em torno de 1, ou **Look-Up Table (LUT)** para o intervalo $[1, 2]$.
- **Erro Máximo:** $\epsilon < 10^{-4}$ bits.
- **Propriedade de Monotonicidade:** O circuito deve provar que se $Q_1 < Q_2$, então $\text{LogApprox}(Q_1) > \text{LogApprox}(Q_2)$.

3. Matriz de Equivalência Semântica

Evento	Comportamento Rust (v1.1)	Comportamento ZK (v1.1 Hardened)
$Q > P$	Retorna Entropy = 0 (Inofensivo)	Prova Inválida (Rejeição Total)
$E < -1.0$	Clamp para 0	Prova Inválida (Range Violation)
$P = 0$	Erro de Execução	Constraint Unmet (Divisão por Zero Impossível)

Conclusão: O circuito ZK é inerentemente mais "agressivo" que o código. Enquanto o Rust tenta salvar a execução, o ZK prefere a "não-existência" da prova perante a incoerência.