

## Axiomatische Gesamtformel (Frames Axiomatics) — Reine Mathematik

\boxed{ \mathcal{F} = \left\langle \mathbf{F}^\*, \sqsubseteq, \tau, \mathrm{enc}, \mathrm{enc}\_\tau, H, \mathcal{A}, \mu, \mathsf{V} \right\rangle \quad \text{mit} \\ \text{Invariante} \quad \mathsf{I}(\mathcal{F}) = \Big( h\_0 = H(\epsilon) \wedge \forall i \geq 1 : h\_i = H \\ \big( h\_{i-1} \mathrel{\mathrm{enc}}\_\tau (\tau(f\_i)) \big) \mathrel{\mathrm{enc}}(f\_i) \Big) \wedge \forall k < \ell : S\_k = \mathrm{prefix}\_k(S\_\ell) }

Kurzbeschreibung (formal):

$\mathbf{F}^* = (f_i)_{i \geq 1}$  ist eine Framefolge;  
 $S_k = (f_1, \dots, f_k)$ .

Die Integrität ist durch die Hashkette  $(h_i)$  gegeben.

Append-only ist die Präfix-Invariante  $S_k = \mathrm{prefix}_k(S_\ell)$  für  $k < \ell$ .