Formal Proof: Hierarchical Threshold Cryptography System

Theorem 1: No Single Tier Sufficiency

Theorem: No single tier alone can reach the threshold $k = 100$.

Proof:

- Tier t_1: Power = $1^2 \times 65 = 65 < 100$
- Tier t_2: Power = $4 \times 18 = 72 < 100$
- Tier t_3: Power = $9 \times 10 = 90 < 100$
- Tier t_4: Power = $16 \times 6 = 96 < 100$
- Tier t_5: Power = $25 \times 3.5 = 87.5 < 100$
- Tier t_6: Power = $36 \times 2 = 72 < 100$
- For tiers ≥ 7: Power = $i^2 \times 2 \times 0.8^{(i-6)}$
  - For tier t_7: Power = $49 \times 2 \times 0.8^1 = 78.4 < 100$
  - For higher tiers, the maximum value occurs at t_9 with 82.944, still below 100

Therefore, no single tier can reach the threshold independently.

Theorem 2: Cross-Tier Collaboration Sufficiency

Theorem: Certain combinations of members from different tiers can exceed the threshold.

Proof: Example 1: 1 member from t_1 and 2 from t_2

- Total power = $65 + (2 \times 18) = 101 > 100$

Example 2: 2 members from t_2 and 7 from t_3

- Total power = $(2 \times 18) + (7 \times 10) = 106 > 100$

Example 3: 5 members from t_3 and 9 from t_4

- Total power = $(5 \times 10) + (9 \times 6) = 104 > 100$

These examples confirm that cross-tier collaborations can successfully exceed the threshold.

Theorem 3: Hierarchical Power Distribution

Theorem: The weight function preserves the hierarchical structure.

Proof:

- $w(t_1) = 65 > w(t_2) = 18$
- $w(t_2) = 18 > w(t_3) = 10$
- $w(t_3) = 10 > w(t_4) = 6$
- $w(t_4) = 6 > w(t_5) = 3.5$
- $w(t_5) = 3.5 > w(t_6) = 2$
- For $i \geq 6$: $w(t_i)/w(t_{i+1}) = 1/0.8 = 1.25 > 1$

Therefore, higher tiers consistently have greater weight per member, maintaining the hierarchical structure throughout all tiers.