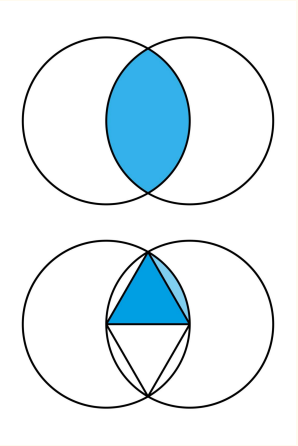
Hierarchical Threshold Cryptography

A System for Enforced Cross-Tier Collaboration

By: Jack Merritt



The Mathematical Problem

How can we design a system that:

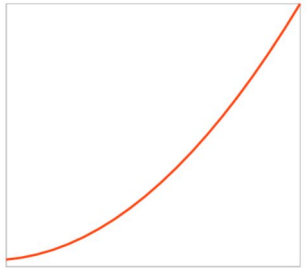
-Mathematically enforces collaboration across organizational levels?

-Prevents any single group from acting unilaterally?

-Preserves hierarchical importance?

Solution: A weighted threshold cryptographic scheme

System Overview at a Glance



Hierarchical Structure: Tiers arranged from t_1 (top) to t□ (bottom)

Member Distribution: Quadratic growth (i^2 members in tier i)

Threshold Requirement: 100 units of "cryptographic weight" needed

Weight Assignment: Higher tiers have more weight per member

Core Result: No single tier can act alone; cross-tier collaboration required

Core Mathematical Concepts

Threshold Function: $T(k) = 100$

-System requires ≥ 100 "weight units" to decrypt

Quadratic Growth Function: $m(i) = i^2$

-Defines member count per tier

Weight Distribution Function: $w(i) = \{...\}$

-Assigns cryptographic "weight" per member

Collaboration Inequality: $\Sigma(m_x \times w(x)) \geq 100$

-Mathematical condition for successful decryption

Tier Structure: Quadratic Growth

The function $\mathbf{m(i) = i^2}$ determines the number of members in each tier:

Tier	Calculation	Members
t_1	$1^2 = 1$	1
t_2	$2^2 = 4$	4
t_3	$3^2 = 9$	9
t_4	$4^2 = 16$	16
t_5	$5^2 = 25$	25

Why quadratic? Creates balanced power distribution

Weight Distribution: Mathematical Definition

- The weight function w(i) is defined piecewise:

$$w(i) = \begin{cases} 65 & \text{if } i = 1 \\ 18 & \text{if } i = 2 \\ 10 & \text{if } i = 3 \\ 6 & \text{if } i = 4 \\ 3.5 & \text{if } i = 5 \\ 2 & \text{if } i = 6 \\ 2 \times 0.8^{(i-6)} & \text{if } i \geq 7 \end{cases}$$

Tier Power Analysis

$$P(i) = m(i) \times w(i) = i^2 \times w(i)$$

Tier	Members (i^2)	Weight per Member	Total Power	Threshold
t_1	1	65	65	< 100
t_2	4	18	72	< 100
t_3	9	10	90	< 100
t_4	16	6	96	< 100
t_5	25	3.5	87.5	< 100

Mathematical Proof: No Single-Tier Decryption

No tier alone can decrypt the message, leading to forced collaboration

- t_1: $P(1) = 1 \times 65 = 65 < 100$
- t_2: $P(2) = 4 \times 18 = 72 < 100$
- t_3: $P(3) = 9 \times 10 = 90 < 100$
- t_4: $P(4) = 16 \times 6 = 96 < 100$
- t_5: $P(5) = 25 \times 3.5 = 87.5 < 100$
- t_6: $P(6) = 36 \times 2 = 72 < 100$

Proof for tiers ≥ 7

For $i \geqslant 7$: $P(i) = i^2 \times 2 \times 0.8^{(i-6)}$

For $i = 7$: $P(7) = 49 \times 2 \times 0.8 = 78.4 < 100$

As i increases beyond 7, **the exponential decay (0.8^(i-6)) outpaces quadratic growth (i^2)**

This means P(i) decreases for $i > 7$

Therefore, no tier $i \geq 7$ can reach the threshold independently

For any collaboration across tiers, the total power is:

$$\mathbf{P\_total = \sum(c\_i \times w(i))}$$

c_i = count of members from tier i participating

$w(i)$ = weight per member in tier i

Decryption succeeds when:

$$P\_total \geq 100$$

Viable Collaboration Examples

Example 1: High-tier focused $P\_total = (1 \times 65) + (2 \times 18) = 65 + 36 = 101 > 100$

-1 member from t_1

-2 members from t_2

Example 2: Mid-tier collaboration $P\_total = (2 \times 18) + (7 \times 10) = 36 + 70 = 106 > 100$

-2 members from t_2

-7 members from t_3

Mathematical Properties of the System

Monotonically Decreasing Weights: $w(i) > w(i+1)$ for all i

-Higher tiers will always have more cryptographic power

Hierarchical Preservation: The ratio between consecutive tiers remains significant

$w(t_1)/w(t_2) = 65/18 \approx 3.6$

$w(t_2)/w(t_3) = 18/10 = 1.8$

For $i \geq 7$: $w(t\_i)/w(t\_\{i+1\}) = 1/0.8 = 1.25$ (constant)

Forced Collaboration:

The threshold k is set such that: $\max\_i (i^2 \times w(i)) < k < \min\_\{i,j\} (i^2 \times w(i) + j^2 \times w(j))$

Geometric Interpretation

The system creates a multi-dimensional space where:

- Each axis represents a tier
- Points represent possible collaborations
- The threshold defines a hyperplane H: $\sum(x\_i \times w(i)) = 100$
- Valid collaborations lie in the half-space beyond this plane
- The piecewise weight function creates interesting geometric properties

https://www.desmos.com/3d/mo7ki5zfjz

System in Practice: Key Properties

Balance of Power: Higher tiers have more individual influence but must still collaborate

Flexible Collaboration: Multiple valid collaboration patterns exist

- Top-heavy: Fewer people from higher tiers
- Bottom-heavy: Many people from lower tiers
- Mixed: Representation across multiple tiers

Adaptability: System works with any organizational size
Mathematical Guarantees: Security properties are provably enforced

Applications in Computational Cryptography

Shamir's Secret Sharing: Extended with weighted participants

- **Traditional:** k-of-n threshold
- **This system:** Weighted threshold with hierarchical structure

Threshold Encryption: Requiring k-of-n participants with weights

Multi-Party Computation: Ensuring balanced input from hierarchical participants

Zero-Knowledge Proofs: Incorporating organizational structure into verification

Practical Applications

Corporate Governance: Secure decision-making across management layers

Multi-Party Computing: Enforced collaboration for sensitive operations

Secret Sharing: Distributed confidential information across organization

Access Control: Sophisticated permission management

Consensus Systems: Weighted voting mechanisms for blockchain/distributed systems

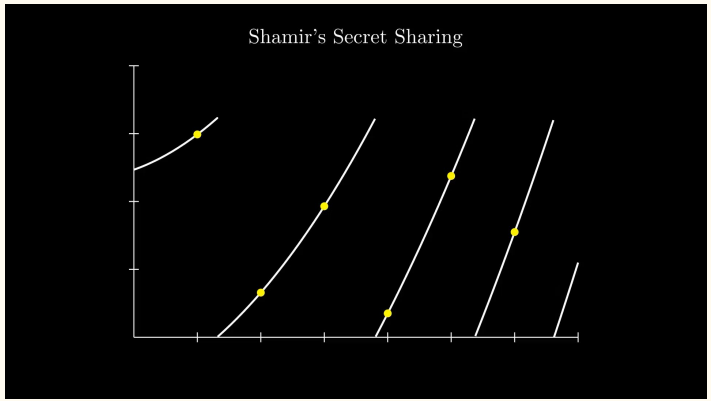
Future Directions

Dynamic Weight Functions: Adjusting weights based on system state

Threshold Optimization: Finding optimal k for specific organizational structures

Multi-Secret Systems: Extending to multiple thresholds for different secrets

Quantum Resistance: Adapting the scheme for post-quantum cryptography



Summary

Mathematical Foundation: Quadratic growth vs. exponential decay creates enforced collaboration

Hierarchical Respect: Weight distribution preserves organizational structure

Provable Properties: No single tier can act alone (proven mathematically)

Flexible Collaboration: Multiple valid patterns for reaching threshold

Practical Applications: Corporate governance, secure systems, access control

Thank you!

Find my contact information at: JackMerrittPortfolio.com