WHITE PAPER / VOLUME 2

Security Analysis: The Mathematics of Memory vs. Brute Force

While traditional security relies on the complexity of characters, SecretMemoryLocker relies on the **entropy of combinations**. To understand why "memory-based keys" are vastly superior to traditional passwords, we must look at probability theory and the *Combinatorial Explosion* effect.

2.1 The Three Tiers of Cognitive Vocabulary

Entropy depends on the size of the "pool" (dictionary) from which words are chosen. We categorize users into three levels of "Personal Entropy":

TIER	DICTIONARY TYPE	EST. VOCABULARY SIZE (N)	DESCRIPTION
Tier 1	Basic	~30,000 units	Common daily vocabulary and basic nouns.
Tier 2	Advanced	~100,000 units	Professional terms, technical jargon, and specific locations.

TIER	DICTIONARY TYPE	EST. VOCABULARY SIZE (N)	DESCRIPTION
Tier 3	Global / Expanded	1,000,000+ units	Unique proper nouns (specific street names, rare book titles, niche hobbies, local context).

2.2 The Comparison: Words vs. Characters

The industry standard for a "strong" password is 12 random characters (including uppercase, lowercase, numbers, and symbols). This provides approximately $94^{12} \approx 4.7 \times 10^{23}$ combinations.

Let's see how SecretMemoryLocker's phrase-based approach compares when using a Global Dictionary pool of 1,000,000 units (10^6):

NUMBER OF WORDS	COMBINATIONS (1M POOL)	SECURITY EQUIVALENCE	BRUTE-FORCE DIFFICULTY
3 Words	10^{18}	~10-11 Complex Characters	Strong (Weeks/Months to crack)
4 Words	10^{24}	> 12 Complex Characters	Infeasible (Millennia)
5 Words	10^{30}	Military Grade / Quantum Resistant	Impossible (Trillions of years)

2.3 The "Personal Entropy" Advantage

The true power of SecretMemoryLocker lies in **Niche Vocabulary**. While a hacker might use a "Dictionary Attack" scanning the top 50,000 most common English words, they cannot easily brute-force a sequence generated from your unique life experiences.

> **Example Chain:**
> `Azazel — Cyberpunk — Prorizna — Oscillograph`

From a mathematical standpoint, this is just a 4-word chain. However, for an attacker, a specific local street like "Prorizna" or a technical term like "Oscillograph" might not even exist in their attack dictionary. By mixing categories (e.g., *Fish Species + Cable Brand + Philosopher's Name*), you create a defense mechanism that renders standard dictionary attacks completely useless.

2.4 Expert Consensus and Industry Standards

Our methodology aligns perfectly with the world's leading cybersecurity authorities:

- **The xkcd Paradigm:** As famously illustrated by Randall Munroe (ex-NASA), the phrase `correct horse battery staple` is significantly harder to crack than `Tr0ub4dor&3`, while being exponentially easier for a human brain to remember.
- **Edward Snowden's Passphrases:** Snowden famously stated that *"passwords are dead; long live passphrases."* He advocates for sequences that make sense only to the user, creating a biological barrier that silicon cannot easily cross.
- **NIST Digital Identity Guidelines:** The U.S. National Institute of Standards and Technology (NIST) has officially shifted its recommendations. They now

discourage forced character substitution (e.g., P@ssw0rd123) in favor of length and memorability, as length is the primary factor in resisting modern brute-force attacks.

- **The Diceware Method:** Our logic mirrors the scientific Diceware system (7,776 words), but expands the entropy pool by orders of magnitude through personal memories and localized data.

2.5 Brute-Force Resilience (The 4090 Metric)

Using a modern hardware setup like an NVIDIA RTX 4090, a standard 12-character alphanumeric password can be cracked in a matter of months. However, a 5-word passphrase drawn from an expanded personal dictionary requires a computing timeframe that exceeds the current age of the universe.

2.6 Multi-Modal Entropy Anchoring (The Bio-Cognitive Synthesis)

While current cryptographic standards rely on either "something you know" or "something you have," SecretMemoryLocker introduces the concept of **Multi-Modal Entropy Anchoring**.

In the conceptual architecture, the "Primary Salt" (currently a file hash) is designed to be replaced by a unique biological or digital anchor. This creates a **Bio-Cognitive Key**, where the final 256-bit hash is mathematically tied to the physical presence of the user.

- **Entropy Fusion:** The master key derivation function (KDF) is expanded to include a physical vector (V_{phys}):

K_{master} = Argon2id(H(*Memories*) $\oplus$ V_{phys}, *Salt, T, M, P*) Where $\oplus$ denotes the XOR entropy fusion of cognitive and physical factors.

- **The Physical Identity Anchor:** This ensures that even if the cognitive sequence (memories) is coerced or guessed, the key cannot be reconstructed without the specific biological or cryptographic signature of the owner.