ENTROKEYLABS™

Predictive Indexing as a Solution to AI and Quantum Threats to Encryption

We *must* secure our information. More than $20T in digital assets are at risk right now. Securing these assets requires reliable encryption, and reliable encryption depends on the ability to generate highly entropic random numbers. There are three basic ways to ensure this happens:

1. The One-time Pad (OTP): provides perfect secrecy by employing a single-use pre-shared key that is larger than or equal to the size of the message being sent.
2. Computational Security: commonly used encryption process which validates entropy by verifying statistical properties such as bit frequency and run distributions.
3. Predictive Indexing: proprietary method of entropy assessment that approaches entropy as a pattern recognition problem and uses Convolutional Neural Networks (CNN) to identify non-linear correlations and hidden structures in large, AI-produced number strings. **Entrokey Labs is the only provider of a software-only, Predictive Indexing solution.**

From an operational perspective, One-time Pad encryption—while nearly impossible to crack if properly implemented—is entirely impractical at scale because of the challenges associated with generating, distributing, and managing an *extremely* large number of single-use keys. Computational Security, on the other hand, has been widely implemented, and the necessary key generation and distribution infrastructures are widely understood and widely used. Predictive Indexing encryption relies on the same key generation and distribution networks as Computational Security solutions. This means there is essentially no logistical challenge to rapid implementation.

In a recent paper entitled *Cryptographic Resilience in the AI Quantum Age: A Predictive Indexing Approach to Entropy Assessment* (available here), Frontier Technologies Laboratory (FTL) at the University of Cambridge looked at how well Computational Security and Predictive Indexing are actually able to evaluate the quality of entropy in a number string, and how well the current entropy standard (NIST SP 800-22) is able to perform the same task (evaluating the quality of entropy in a number string). The paper highlights three key findings.

First, traditional Computational Security tests to validate entropy focus on the concepts of Shannon Entropy and Min-Entropy to quantify the quality of an entropy source. Unfortunately, FTL's researchers found that measurements can validate a number string as having perfect (1.0 on a scale of zero to one) Shannon Entropy, but actually have zero conditional entropy (the amount of information needed to predict the next number in a series). This result: the entire future sequence of numbers can be predicted after observing just 624 consecutive 32-bit outputs.

Second, by using an AI diffusion model to generate multiple random number candidates and selecting the best using Predictive Indexing, Entrokey Labs' solution is able to achieve consistently high quality entropy (0.9484 on a scale of zero to one), and to measure it continuously. This is made possible because the CNNs employed by Entrokey's solution are able to identify non-linear correlations and hidden structures in the data that are not visible to Computational Security entropy tests.

Finally, FTL found that current NIST standards—notably NIST SP 800-22 and its successor, SP 800-90B—rely on traditional, Computational Security approaches and a pass/fail approach to entropy validation. This approach aligns with Shannon entropy, and results in passing assessments that do not necessarily guarantee cryptographic security. AI and quantum vectors can and do find patterns in strings that pass NIST SP 800-22 and 800-90B.

Armed with this knowledge, we can see three imperatives. First, if we want our data to be secure, we *must* upgrade our information security, and that means we *have* to take a different approach to encryption. Predictive Indexing is that approach. Next, if we want to stay ahead of the threat vectors represented by AI and quantum computing, we *must* move quickly. This means that we cannot wait for design, testing, integration, production, installation, and re-testing of hardware-based solutions. Only a software-only solution can meet the urgency placed on us by our adversaries. Entrokey Labs provides the only solution that meets both of these imperatives. Finally, we *must* change the standards by which we evaluate entropy; we can no longer measure against what's worked in the past…we must measure against the threat we face now and in the future!