EXPANSE LABS

DEFEAT QUANTUM COMPUTING

Using linear measurements on physical tokens allows us to defeat quantum computing. While no encryption system is truly immune to brute force decryption, our technology allows a new key to be used for each transmission. This means only one message is revealed when a key is cracked, not a large group of communications. Since even quantum computers take time to decrypt a message, our technology shifts the cost/benefit balance strongly in our favor.

Of particular relevance is the ability to indirectly transmit encryption keys. Any key, no matter how long, can be split into segments which fit into the measurable space on a token. This allows a temporary key of the same size as the base key to be generated from the token, providing the perfect security of a one-time pad for the transmission of a new base key. Using our standard tokens, a 5.12” maximum working length corresponds to a 9-bit chunk, so you can send a 256-bit key with 29 measurements. This lets you transmit keys with absolute security even over unencrypted transmissions to reestablish quantum-resistant symmetric encryption.

Furthermore, our technology is highly adaptable. It is agnostic to the key length so it can be applied to new encryption algorithms as soon as they are developed. The ability to easily modify our algorithm also allows parameters to be updated along with the base key to further improve security. This keeps our technology relevant against constantly evolving threats.

Adoption is simple and low cost. Enterprises can retain full control of the system and avoid paying third party fees. Contact us for purchasing and licensing options.