XOTIC®

The Future of Agile Cryptography

Engineered to protect today's emerging technologies

Agile enough to encrypt ANYTHING

THE NEED FOR AGILE CRYPTOGRAPHY HAS NEVER BEEN GREATER

- Vast majority of current software & hardware products are hard-coded to work with a single algorithm
- Investments in Quantum Computing are driving demand for new Post-Quantum cryptography
- Financial penalties associated with not implementing encryption continue to increase
- Cybercriminals are now stealing encrypted data for decryption in the future
- Increased regulatory compliance around data protection and privacy
- Emerging technologies are having to use less secure or no encryption
- Most open source and standardized encryption in use is 20yrs+ old
- Increase in data retention/ archiving for use by Big Data Analytics

XOTIC CRYPTOSYSTEM DESIGN

XOTIC is a One-Time Pad style hybrid streaming symmetric cipher. The design requirements for XOTIC were based on the following set of criteria important to enterprise organizations looking to increase their security posture, manufacturers looking to secure emerging technologies and IoT devices, and applications developers who would benefit from licensing and implementing crypto-agile encryption today:

- Investment & future-proof protection of encrypted data
- Portability and adaptability for use in low-power/compute or memory/bandwidth-constrained platforms

IDENTIFIED USE CASES FOR XOTIC

- Email/IM
- Voice/ Videoconferencing
- Consumer Devices/ Technology
- RDBMS/ NoSQL/ Big Data
- Blockchain
- On-Prem Storage
- Cloud Storage Environments
- Cloud Backups/ Archive
- Software-Defined Networking
- Device-to-Device Transfers
- IoT Security
- Device-to-Device
- eCommerce/ Web Apps
- Regulation Data (GDPR/ HIPAA/ Others)

XOTIC CRYPTOSYSTEM ATTRIBUTES

THE BENEFITS ARE CLEAR

Efficiency - Time to initialize and begin encrypting is faster than streaming ciphers or AES using dedicated (NI) hardware instructions sets.

Operation - Performance metrics exceed ChaCha20 or AES in software implementations

Secure Channels will support the newest Advanced Vector Extensions (AVX) which have been shown to significantly accelerate cryptographic processing time and will deliver a significantly increase to XOTIC's already excellent performance.

Strength - The encryption key space can be easily extended using a Dial Setting, (Dial-1 = 512-bit, Dial-2 = 1,024-bit... Dial-9 = is 131,072-bit "Archive Strength") Only uses QRNG or CSRNG sources of entropy for maximum security.

Extensibility - Coded in C++, JAVA, and Python for use emerging technologies (IoT, Device-to-Device, Automobile BUS architectures, as well all existing O/S, application, hardware, and cloud implementations.)

Adaptability - Extremely small and lightweight footprint make it ideal for compute/ memory/ power/ bandwidth/ space restrictive environments including: FPGA's, ASIC's, Raspberry Pi, ARM/Mobile.

Attack Resistance - A new secret key is generated for every encryption process and the encryption changes dynamically from one process to another. When queried, it will always produce a positive response making (negative-response) Brute Force attacks ineffective.

Key Management - Agnostic compatibility with existing symmetric key management appliances or services including the Amazon Web Services (AWS) key management service.

Also compatible with newest, non-PKI, alternative key exchange process from Secure Channels, the Secure Key Infrastructure (SKI). SKI leverages existing highly-available worldwide distributed satellite networks from AWS, Azure, or others. (Additionally information found in SKI White Paper.)