The Whisper Company

Chaotic Hybrid Encryption

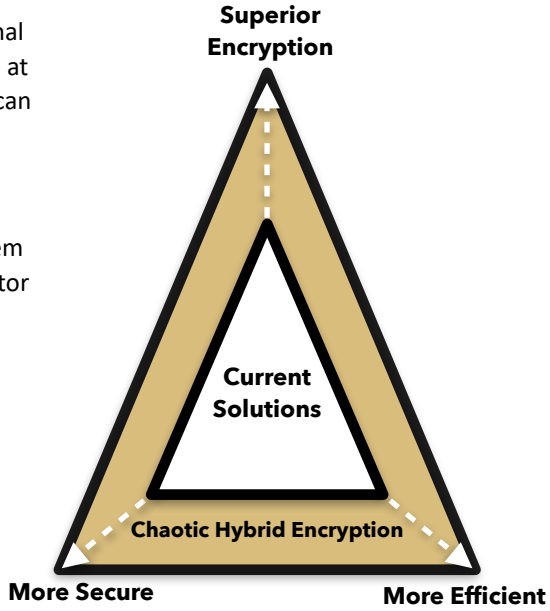
Quantum-Resistant Encryption

The next generation of data security via "quantum-resistant" encryption, called **Chaotic Hybrid Encryption (CHE™)**. CHE is a patented technology that merges hybrid (mixed-signal) computing and chaotic oscillators to provide an infinite pseudo-random number generator (PRNG) for a one-time pad (OTP) in-line encryption that is 20-100 times after than current military grade encryption.

CHE™ Technical Glance

The **CHE**™ (**C**haotic **H**ybrid **E**ncryption) is an environment that enables developers to embed in their apps in-line encryption that is "quantum-resistant". The SDK/API can also provide a **PRNG** (**P**seudo-**R**andom **N**umber **G**enerator), named **∞Key**™ (InfiniKey) that is used by CHE for a **OTP** (**O**ne-**T**ime **P**ad) unbreakable encryption.

The CHECK™ (Chaotic Hybrid Encryption Computing Kit) :



- Emulates UT's patented **HxC** (**H**ybrid e**X**treme **C**omputer), a mixed-signal integrated circuit capable of simulating nonlinear differential equation at speeds between supercomputers and quantum computers. The user can select via a **KGK** (**K**ey-**G**enerating **K**ey) the parameters for the HxC emulation.
- The **HxC** simulates chaotic oscillators (**ChaOs**). There is a library of chaotic oscillators available to chose from and the user can extend them with their own classes. The KGK is used to select which chaotic oscillator is being used and at which time (when and how to switch them). Associated with the "selected" chaotic oscillator, the KGK has the coefficients of the oscillator and the initial conditions, or ranges for random selection.
- A **P**seudo-**R**andom **N**umber **G**enerator (**PRNG**) algorithm–termed ∞Key™ (InfiniKey)– creates an infinite bitstream (sequence of bits "1/0", that satisfies NIST randomness tests) as needed by the encryption. It may use all the information from the HxC states of the ChaOS, the reset times of the HxC, and parameters of both HxC and ChaOS. The KGK selects the ∞Key parameters.
- The last step is the **C**haotic **H**ybrid **E**ncryption (**CHE**™) algorithm to be used. Since the ∞Key generates a seamlessly true random number, even a simple XOR should work, but the user may select among several encryption algorithms like AES (Advanced Encryption Standard) , RAS, DES, Skipjack, etc. with a *Mode* that accommodates the use the OTP resulting from the ∞Key.

KGK: [HxC : ChaOs : PRNG : CHE]

The Key-Generation Key (KGK) provides:

- The HxC: operating conditions (time step, thresholds, bits, reset logic, etc.)
- The ChaOs: (type of chaotic oscillator, coefficients, initial conditions, etc.)
- The ∞Key: (Confusion/Diffusion algorithms, PRNG methods, context selection, etc.)
- The CHE: (methods of encryption, scheduler, etc.)

The encryption key is generated locally (no key distribution) with no hardware expenditure and reduced overhead.