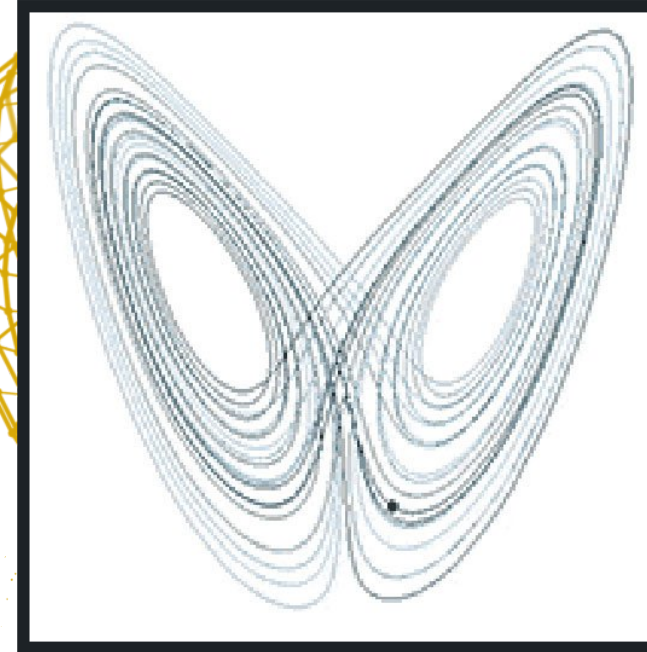


SAFEGUARD YOUR ENTERPRISE DATA WITH QUANTUM SECURE ENCRYPTION 3

The world is changing. Classical encryption methods are vulnerable to attacks by quantum computers. Businesses and governments need to protect against these threats, increase their security posture and secure communication methods so that they can withstand quantum attacks.

LET'S TALK

FOR DEVELOPERS



1

THE THREAT

THE QUANTUM COMPUTING THREAT IS REAL &
IT IS HERE NOW

2

WHY NOW

HNDL ATTACKS ARE HERE

Not in 10 years, Today. Nation state adversaries and other attackers are harvesting data now and planning for the future. You need crypto agile solutions to be ready.

Harvest Now, Decrypt Later (HNDL) attacks steal your encrypted data now and decrypt it later when a quantum computer is available.

[READ MORE](#)

Deloitte.

“Half of organizations believe they are at risk for ‘Harvest Now, Decrypt Later’ cybersecurity attacks.”

– Deloitte

3

BY THE NUMBERS

0

“Every 39 seconds a hacking takes place worldwide”
– Security Magazine (2020)

\$0M

“Global average total cost of a data breach”
– IBM Cost of a Data Breach Report (2022)

85

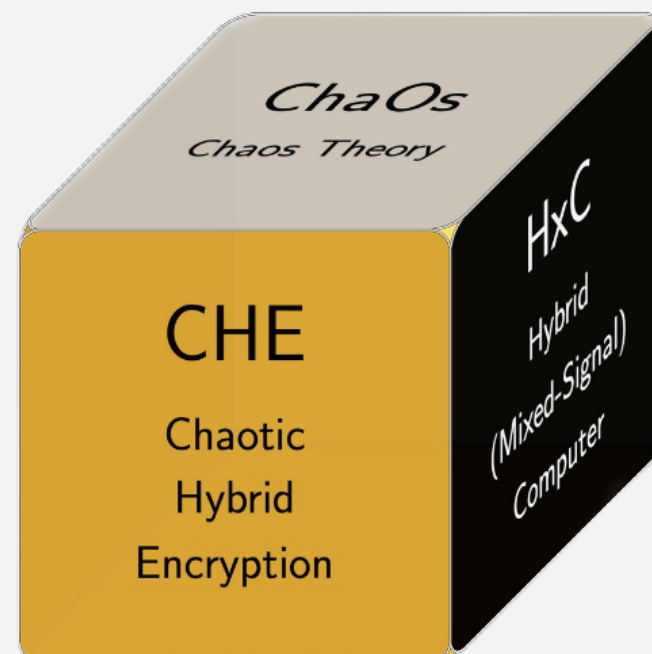
“85% of attacks are now utilizing encryptions for their channels”
– Help Net Security

53

“53% of companies left 1,000+ sensitive files unencrypted”
– Global Data Risk Report

4

A NEW TECHNOLOGY PARADIGM



QUANTUM-SECURITY-AS-A-SERVICE

In a novel way, we leverage chaos theory and a hybrid (Mixed-Signal) computing paradigm in our products to create more powerful and efficient entropy, truly random and infinite keys, and unbreakable quantum-proof encryption.

OUR TECHNOLOGY BENEFITS

- **Speed** – Ultra fast speed. 20 -100x faster than alternatives
- **Efficiency** – Low overhead. Saving time and money.
- **Localized** – More secure. Zero Sharing. Zero Trust.
- **Zero Hardware** – No Expensive Specialized Hardware

9

CHE DIMENSION

- ∞ Key Generator
- Symmetric vs. Asymmetry
- Block vs Stream

CHAOS DIMENSION

- ChaOs Set
- Coefficients Map
- Initial Conditions
- Manifolds Guards

HXC DIMENSION

- Mantissa/Exponent
- AnalogBit / Cup Size
- Time Step
- Periodicity

KGK: KEY GENERATION KEY

A NEW TECHNOLOGY PARADIGM

QUANTUM-RESISTANT SUITE

CHAOTIC HYBRID ENCRYPTION

CHAOTIC HYBRID KEY GENERATION

CHAOTIC ENTROPY

CHAOTIC HYBRID ENCRYPTION

Developers need familiar tools based on modern development practices. We provide an SDK that can easily be integrated to applications and infrastructure to make them quantum-secure.

KEY POINTS:

- With an ∞ Key, we can do a OTP (One-Time Pad) encryption-as simple as an XOR- that is Quantum-Resistant.
- The Chaotic Hybrid Key Generation is local, so no ∞ Key is ever transmitted or shared, reducing the vulnerability of the system.
- Since only the algorithm itself is purview to the ∞ Key, this is a realization of Zero-Knowledge Encryption

BENEFITS

- Quantum Resistant
- No Specialized Hardware Needed
- Highly Efficient, saving computing cost
- Speed

10

REQUEST A DEMO

TALK TO SALES

IMPLEMENTATION



EMBEDDED IN CLIENT'S APPLICATION

- SDK is Embedded. The Encryption Key is generated and stays in the app. Zero Knowledge Encryption. The key is never shared, unlike competitors using micro services.
- The client/developer adds the CHE functionality in the application itself. There is no community outside the SandBox where the App lives.



LAN SERVICE WITHIN THE ENTERPRISE FIREWALL

- API Service Solution is where the entropy generation, ∞ Key, and CHE are performed within the enterprise firewall
- A local server within the LAN (Local Area Network) provide the service
 - Entropy Generation
 - Random Number Generation
 - Chaotic Hybrid Encryption/Decryption



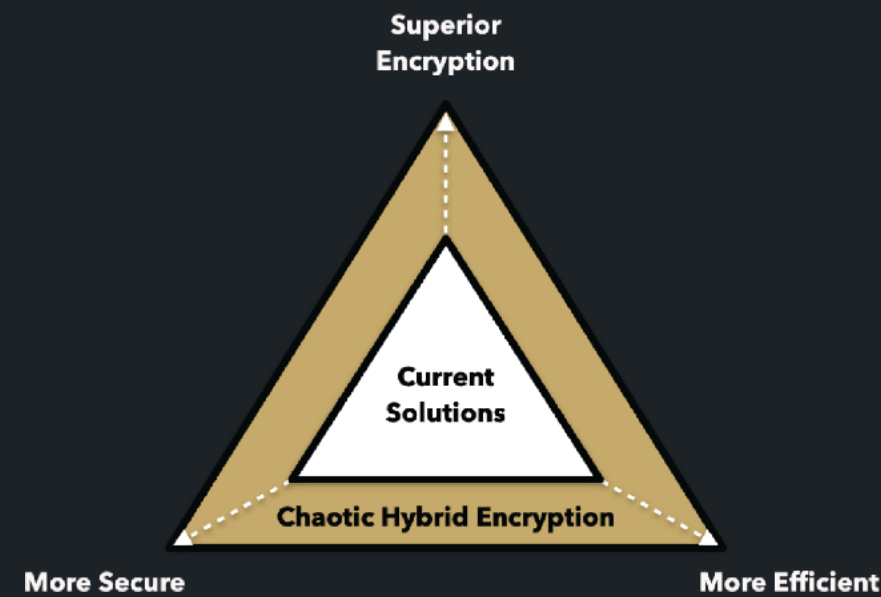
GOOD ENTROPY AND RANDOM NUMBERS SOURCE PLATFORM

- In this solution the entropy generation, ∞ Key, and CHE are performed in the cloud.
- This solution is more suitable for enterprises with large data servers that want to re-encrypt their data and make it quantum proof.

11

CHAOTIC HYBRID ENCRYPTION

Our novel Chaotic Hybrid Encryption (CHE) is future-proof everlasting encryption that is easy to implement and cheaper than other quantum-proof alternatives. It's more secure, more efficient and better (unbreakable) encryption than the current standard. It is truly random, requires no expensive specialized hardware, and is localized (Zero Key Distribution).



SUPERIOR ENCRYPTION

- Zero Knowledge Encryption. Even developers don't know keys.
- ∞ Key – InfiniKey. Cypher is as long as the message.
- One-Time-Pad Encryption. Unbreakable Encryption.
- Chaos Theory generates truly random numbers.



MORE SECURE

- Localized. Reduce attack surface area and risk of MITM attacks.
- Zero Key Transmission. No sharing of keys over the network.
- Quantum Resistant. Long term security from HNDL attacks.
- Patented Technologies that Exceed Federal NIST mandates.



MORE EFFICIENT

- Ultra Fast (10-100x Faster than than military grade encryption)
- No Expensive Specialized Hardware. Easy to integrate SDK.
- Less Overhead. Less clock cycles = reduced encryption costs.
- Overcome limitations of Quantum Key Distribution. No Fiber needed.

5

CURRENT SOLUTION SHORTCOMINGS

COMPETITOR'S PROBLEMS

Expensive and Inefficient



Hardware: Quantum specific hardware & fiber optics are costly, expensive to install and have limitations on distance.



Current solutions require many cycles of cpu usage, racking up costs.

vs

OUR SOLUTION

Inexpensive and Efficient



No specialized hardware needed

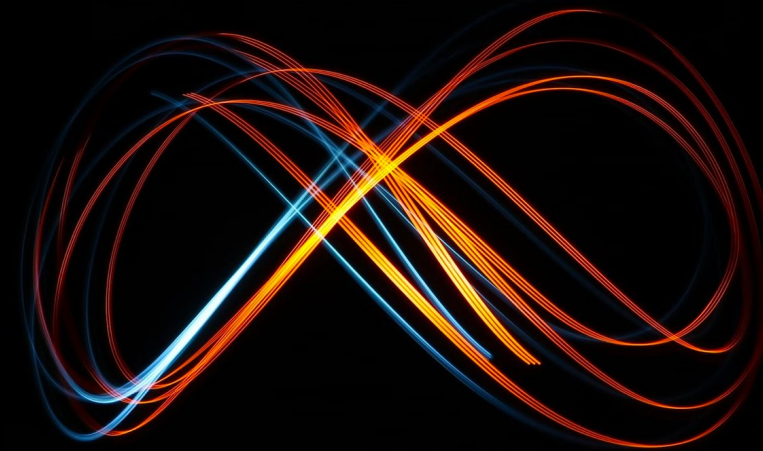


Infinikey reduces clock cycles, cpu usage, and cost/price

6

HOW LONG SHOULD A STRONG ENCRYPTION
KEY BE? ... 256? 512? 1024?

OUR KEY IS
INFINITE



12

TECHNOLOGY COMPONENTS

CHE

- High Level Description
- One-Time Pad Encryption/Decryption can be XOR = 25+ times faster than AES

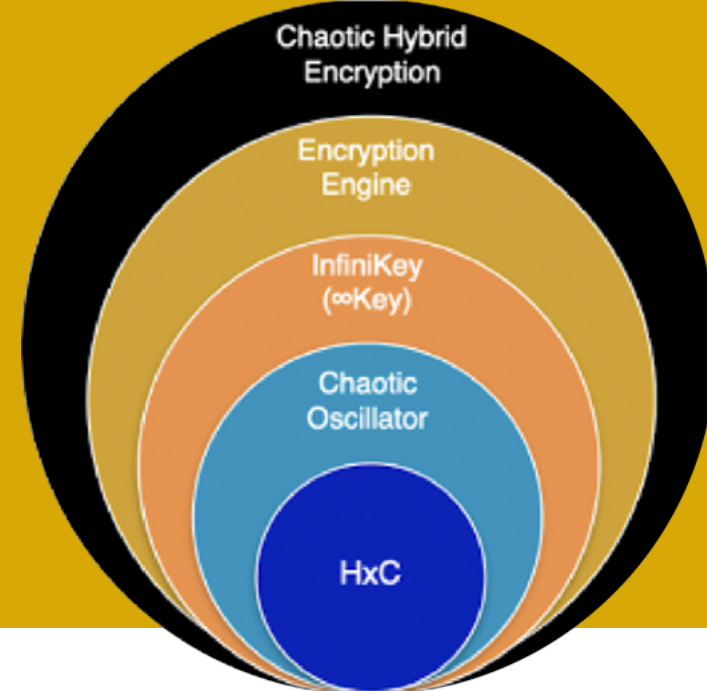
INFINIKEY

- High Level Description
- InfiniKey, generates an infinite chaotic bitstream (pseudo-random number generator - PRNG)

CHAOS

- High Level Description

13



- Never repeats, cannot e inverted — confusions & diffusion

HYBRID (HXC) COMPUTING

- High Level Description
- Speeds between Supercomputer & Quantum Computer

VERTICALS & APPLICATIONS



GOVERNMENT



BANKS



DATA CENTERS



HEALTH CARE



TELECOM



DEFENSE



AUTOMOBILES



BFSI



CRITICAL
INFRASTRUCTURE



HIGH TECH INDUSTRY

REQUEST A DEMO

TALK TO SALES

8

USE CASES

SECURE TRANSFER OF SECRETS, KEYS AND CREDENTIALS

Protect sensitive information that needs

SECURE MULTI CLOUD AND HYBRID CLOUD TRAFFIC

Sending data between cloud
environments across multiple clouds

PROTECT INTELLECTUAL PROPERTY

Whether transferring data to factories
or cloud, protect sensitive information

Protect connectivity of services that send and receive secrets from key management systems to secure your most critical data.

environments, networks, or regions? Ensure that your most sensitive data is

abroad or just between remote offices and child storage, protect your enduring intellectual property.

protected from a man-in-the-middle attack.

PROTECTING KEYS = PROTECTING DATA

Whenever you're moving data, quantum securing your keys immediately enhances data security

PROTECT PII PERMANENTLY

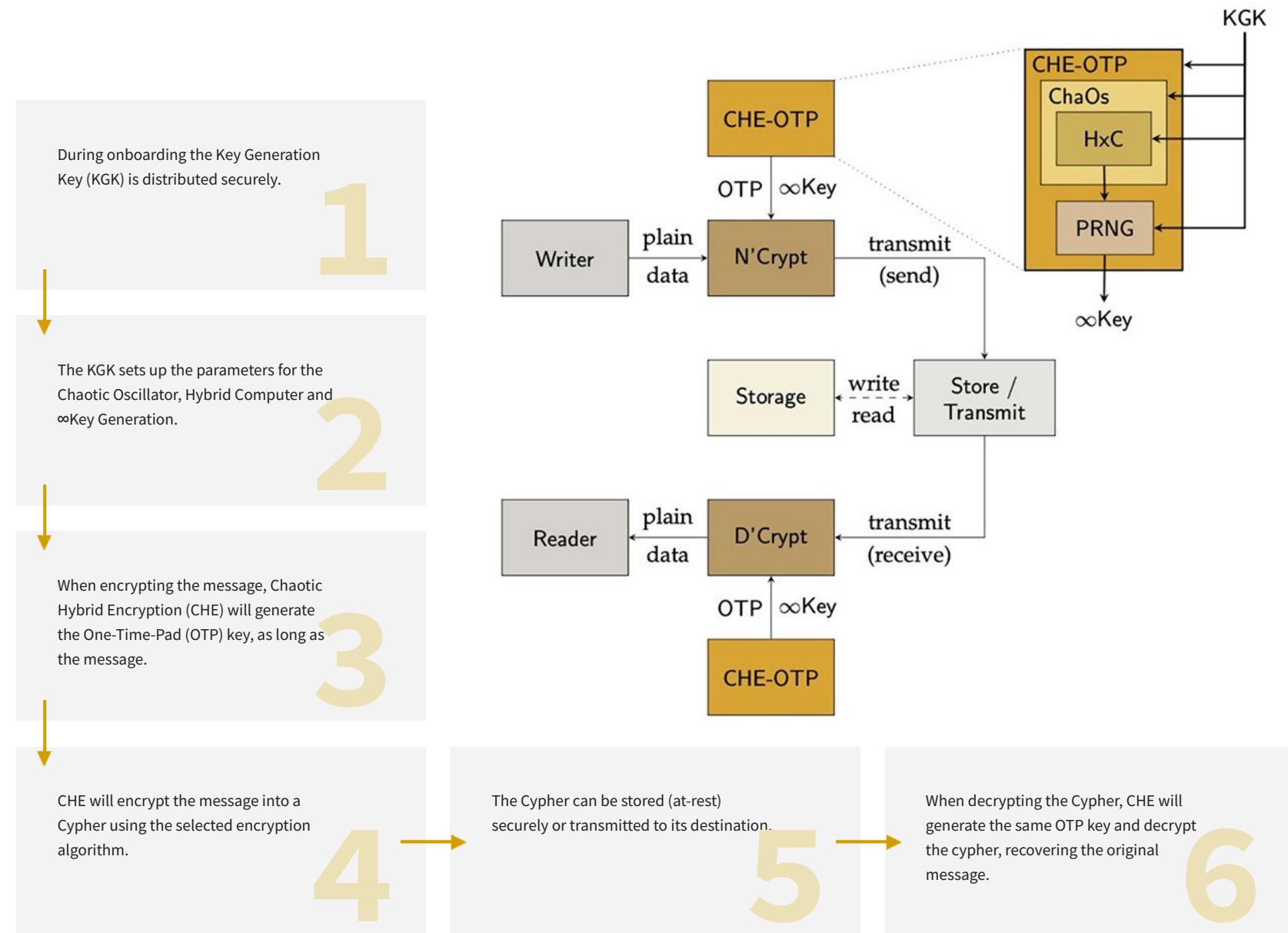
DNA data and other personal information have a value that needs to live beyond when quantum computers break RSA and AES encryption. Save your data's value now.

REDUCE CRYPTO-AGILITY COSTS AND RISK

When RSA, AES or any algorithm fails, your captured data is exposed. Protect important data once and for all.

7

TECHNOLOGY IMPLEMENTATION



14

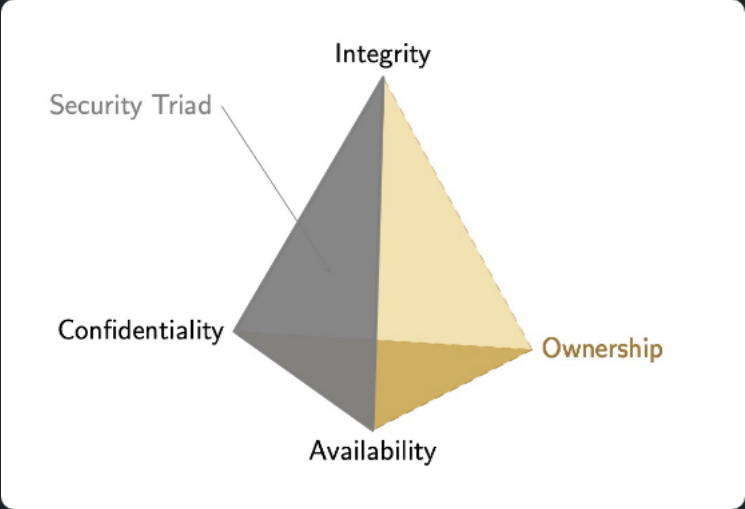
GET STARTED

TRUE DATA SECURITY: OUR MANIFESTO

CIAO – ADDING OWNERSHIP
TO THE SECURITY TRIAD

The security triad, CIA, has three components: Confidentiality, Integrity and Availability. We believe that it is time to change the paradigm and add a fourth dimension, Ownership (CIAO). We believe that private and secure communication is a human right. And that ownership is at the heart of privacy and security.

“CIAO MANIFESTO



15



[PUA Framework](#)

[CHE API](#)

[The Invisible Ink App](#)

[Our Technology](#)

[About Us](#)


[Privacy Policy](#)

[Terms and Conditions](#)

[EULA](#)

[TINDA](#)

[Do Not Sell My Personal Info](#)

 info@thewhispercompany.com



Copyright © 2022. The Whisper Company. All Rights Reserved