Patented

CHAOTIC HYBRID ENCRYPTION

SAFEGUARD YOUR ENTERPRISE WITH QUANTUM SECURE ENCRYPTION

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.

HARVEST NOW DECRYPT LATER (HNDL) ATTACKS ARE HERE

Today, not in 10 years, nation states, adversaries and other attackers are harvesting data now and planning for future decryption. We need crypto agile solutions for protection.

Harvest Now, Decrypt Later (HNDL) attacks are the stealing of encrypted data today with plans of decrypting it with quantum computing. Once this day happens, adversaries will have access to sensitive PII, trade secrets and other private and confidential information that today we consider "safe".

Deloitte.

"Half of organizations believe they are at risk for 'Harvest Now, Decrypt Later' cybersecurity attacks."
— Deloitte

MIT Technology Review

"The threat is that they copy down your encrypted data and hold on to it until they have a quantum computer."
— *MIT Technology Review*

BCG BOSTON CONSULTING GROUP

"Data currently transmitted (…) is vulnerable to 'store now, break later' attacks since public internet traffic is easily duplicable."
— *Boston Consulting Group*

NCI AGENCY
NATO Communications and Information Agency
Agence OTAN d'information et de communication

"Securing Nat's Communications from the quantum era is paramount to our ability to operate effectively without fear of interception. With the threat of harvest now and decrypt later looming over secure communications, this is an increasingly important effort to protect against current and future threats."
— *Konrad Woran, Principal Scientist, NATO Cyber Security Centre*

CURRENT SOLUTION SHORTCOMINGS

COMPETITOR'S PROBLEMS

EXPENSIVE & INEFFICIENT

- ✕ QUANTUM SPECIFIC HARDWARE & FIBER OPTICS ARE COSTLY, EXPENSIVE TO INSTALL AND HAVE LIMITATIONS ON DISTANCE.
- ✕ CURRENT SOLUTIONS REQUIRE MANY CYCLES OF CPU USAGE AND LATENCY, RACKING UP COSTS.

DETERMINISTIC

- ✕ MOST RNG (RANDOM NUMBER GENERATORS) ARE DETERMINISTIC AND CAN BE VIOLATED.

KEY TRANSMISSION

- ✕ ENCRYPTION KEYS & DATA IS BEING CAPTURED TODAY. KEY TRANSMISSION IS AN INHERIT VULNERABILITY.

VS

OUR SOLUTION

INEXPENSIVE & EFFICIENT

- ✓ NO SPECIALIZED HARDWARE NEEDED. REDUCING UPFRONT COST WITH LITTLE INSTALL COSTS AND NO LIMITATIONS ON DISTANCE.
- ✓ INFINIKEY AND ONE-TIME PAD (OTP) ENCRYPTION REDUCES CLOCK CYCLES, CPU USAGE AND COST.

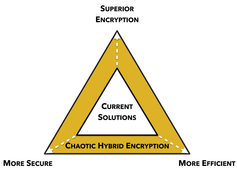
CHAOTIC

- ✓ CHAOTIC SYSTEMS WITH HXC (HYBRID EXTREME COMPUTING) ARE NOT DETERMINISTIC AND CAN'T BE VIOLATED.

ZERO KEY TRANSMISSION

- ✓ KEYS ARE GENERATED AT EACH ENDPOINT & NO KEYS ARE TRANSMITTED. ZERO-KNOWLEDGE ENCRYPTION.

OUR SOLUTION: CHAOTIC HYBRID ENCRYPTION



Our novel Chaotic Hybrid Encryption (CHE) is future-proof everlasting encryption SDK 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

- 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 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.

✓ MORE SECURE

- 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.

EXAMPLE USE CASES

SECURE TRANSFER OF SECRETS, KEYS AND CREDENTIALS
Protect connectivity of services that send and receive secrets from key management systems to secure your most critical data.

SECURE MULTI CLOUD AND HYBRID CLOUD TRAFFIC
Sending data between cloud environments, networks, or regions? Ensure that your most sensitive data is protected from a man-in-the-middle attack.

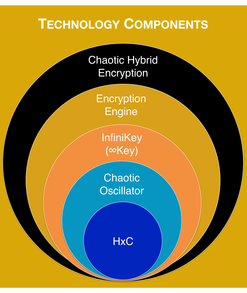
PROTECT INTELLECTUAL PROPERTY
Whether transferring data to factories abroad or just between remote offices and chilled storage, protect your enduring intellectual property from quantum hacking.

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.

TECHNOLOGY COMPONENTS



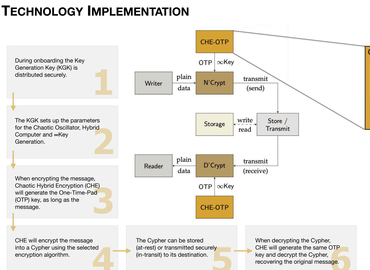
CHAOTIC HYBRID ENCRYPTION
- ONE-TIME PAD ENCRYPTION/DECRYPTION CAN BE XOR (25X FASTER THAN AES)

INFINIKEY (∞KEY)
- INFINIKEY, GENERATES AN INFINITE CHAOTIC BITSTREAM (PSEUDO-RANDOM NUMBER GENERATOR - PRNG)

CHAOTIC OSCILLATOR
- NEVER REPEATS, CANNOT BE INVERTED - CONFUSION & DIFFUSION

HYBRID (HXC) COMPUTING
- SPEED BETWEEN SUPERCOMPUTER & QUANTUM COMPUTER

TECHNOLOGY IMPLEMENTATION



CHE Patent No. US 9,853,809