Qrypt

vaultree
Privacy is our nature

The new world of absolute privacy.

Quantum-Secure Proxy and Key Generation

Key benefits

- Generate identical keys at multiple endpoints
- Never distribute encryption keys over an insecure channel
- Protect against harvest now decrypt later quantum attack

Vaultree and Qrypt – Real-time Searchable & Fully Homomorphic Encryption together with Quantum-Secure Keys without Transmission

Vaultree provides fully encrypted data processing without compromising performance. Enabling processing of atomic portions of data, Vaultree integrates into any common technical enterprise stack with the highest use case variety. With Qrypt’s ability to independently generate identical symmetric keys at multiple endpoints and quantum-secure future-safe one-time pad encryption, Vaultree and Qrypt are making fast, future secure data processing in a cloud-first world possible.

The Challenge

Security of encryption keys is critical. Adversaries with unlimited resources are attacking key distribution and data transmission, harvesting keys and encrypted data. With the advent of quantum computers, they will have access to today's data and keys, exposing you to unfathomable risk. Any algorithmic approach to encrypting data in transit, like asymmetric encryption, and even NIST post-quantum computing (PQC) algorithms, are not proven quantum-secure. Late last year, a second-round NIST PQC submission was proven insecure; once quantum computers are available and with improvements in machine learning (ML), it won't be surprising if other weaknesses emerge to render encrypted data exposed.

The Solution

Qrypt's Secure Proxy solution for Vaultree enables a quantum-secure one-time pad (OTP) encrypted proxy tunnel to secure the transmission of keys between your client and the HashiCorp Vault. OTP encryption is information-theoretic security, making OTP-protected data everlasting secure - mathematically proven safe against all known attacks, including future quantum computers.

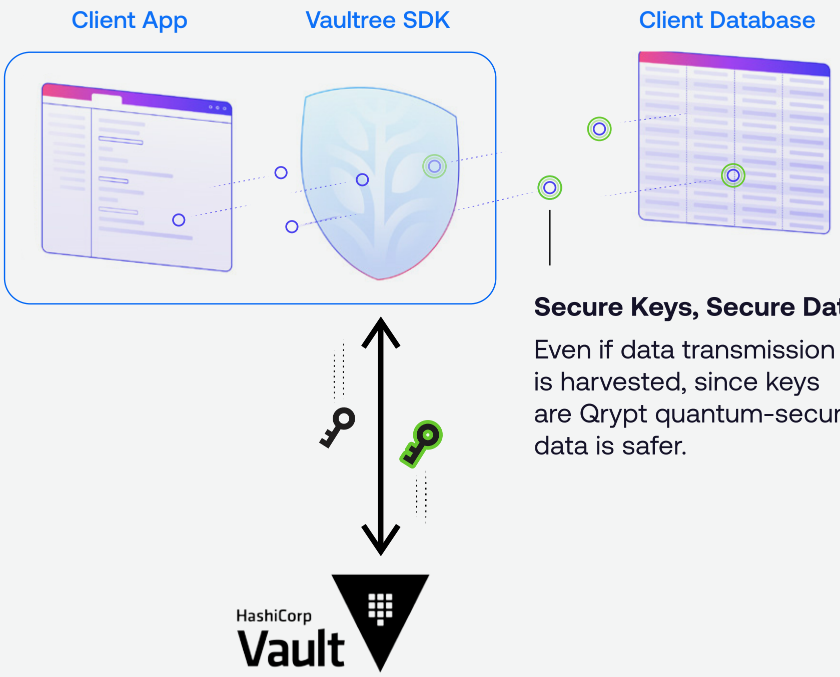
Additionally, Qrypt Key Generation, leveraging patented algorithms and peer-reviewed encryption techniques, permits identical keys to be securely generated at multiple endpoints eliminating the need for key distribution.

Secured by
Qrypt

Everlasting Key Security

Today's key transport is done in TLS secured proxy. TLS is at risk from future quantum computers.

With Qrypt secure proxy, even harvested data is quantum-secure. Keys are protected forever.



Secure Keys, Secure Data

Even if data transmission is harvested, since keys are Qrypt quantum-secure, data is safer.

Entropy

The Qrypt Entropy service is the foundation of all Qrypt solutions. The Entropy service streams random numbers extracted from a diversified set of high-quality quantum phenomena sources. By having multiple source phenomena, the system gains redundancy and protection against potential future analysis that may prove any one source characterizable or vulnerable to attack, making the overall service more reliable and secure.

The Entropy service is robust and can provide random for even the most demanding communications and data transfer solutions.

Attacks on Random Number Generators

Random numbers are incredibly valuable in use cases, including cryptography, optimization, gaming, simulation, statistical sampling, etc. Many of the random numbers in use today aren’t random at all — they just appear to be. Generated using a computational algorithm based on a short seed or based on a physical measurement, such as the thermal noise of a resistor, many have characterizable patterns. If somebody can guess a seed, then they’ll be able to predict future random numbers. There are also attacks that have demonstrated that you can characterize physical sources and begin to guess random numbers.

The implication for cryptography is that with weak random the encryption isn’t as secure as it seems.

Qrypt

www.qrypt.com

Getting started

Go to portal.qrypt.com/register to create your account, generate your token, and begin downloading high quality entropy in minutes.