Qrypt

Qrypt Quantum Security

Stop transmitting encryption keys.

- *Encryption keys and data are being harvested today.*
- *Data in motion and at rest will be compromised when harvested keys are decrypted.*
- *Risk must be remediated ahead of a lengthy Post-Quantum Cryptography (PQC) migration*

Transmitting encryption keys is a fundamental security vulnerability. When using cryptographic algorithms like RSA and NIST Post-Quantum Cryptography (PQC), the session keys used to encrypt your data during transmission are being transmitted. While we can assume data transmitted is secure over the short term, the risk stems from the fact that over the long-term algorithms eventually fail. When they do, every byte of data transmitted to that date will become immediately vulnerable and exploitable. RSA will fail due to quantum computers, and we don't know how long before the PQC algorithms fail.

If you don't eliminate key transmission, you don't eliminate the risk—even with PQC.

Encryption is one of your strongest weapons against threats to your sensitive data, intellectual property, and private communications. Even if you think you have the strongest encryption in place, there's still plenty for proactive CISOs to worry about. Ongoing nation-state threats. Key management complexity. Government security mandates. Present danger and risk of harvest now, decrypt later attacks. Need for truly random, high entropy key generation. Costs and vulnerabilities associated with fail and replace encryption strategies. And, of course, the root cause of today's post-quantum crisis— the key transmission vulnerability.

With so many current worries and challenges on your plate today, you might believe improving key transmission security is something that can be delayed to the future. But solving key transmission security addresses serious risks that all organizations face today and protects against the future quantum threat. Transmitting keys is a foundational risk to security as keys and data are harvested for decryption later. If that foundation crumbles, so do all your protections.

For example, every byte of data you encrypt today with RSA, or even post-quantum cryptography (PQC) algorithms, will become immediately vulnerable and exploitable when those algorithms eventually fail. You can't simply re-encrypt that data to secure it. Much of it will already be in the wild. Nation-states and organized crime make it an ongoing practice to collect encrypted data so they can decrypt it in the near future. In fact, in a single operation, China siphoned "hundreds of gigabytes of intellectual property and sensitive data"[1] from organizations in the manufacturing, energy, and pharmaceutical sectors.

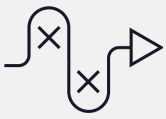
Qrypt Quantum Security provides your organization the strongest encryption foundation available to address the security challenges and risks you face now, by remediating today's key transmission vulnerability. It's available on-demand as-a-service, on-premises, on any device, and is as simple to deploy as a drop-in container or four lines of code.

Qrypt Quantum Security Suite

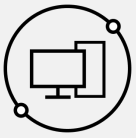
Qrypt's unique ability to achieve security derives from the synergistic interaction of its foundational technologies and products that can address the depth and breadth of your varied security challenges. The Qrypt Quantum Security Platform makes it easy for you to leverage these technologies and products in your existing internal systems or business applications. Whether you're building from scratch or surgically remediating the key transmission vulnerability today, Qrypt makes it easy.

Qrypt secures long-term sensitive data with permanent encryption, such as biometric markers, covert intelligence asset identities, Social Security IDs, and weapon designs.

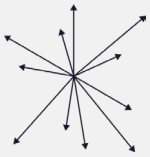
Quantum
Key Generation



Quantum
Secure Tunnel



Quantum
Secure Encryption



Quantum
Entropy

Quantum Random
Number Generators

BLAST
Protocol

Our platform technologies enable extraction of keys from pools of random numbers derived from quantum measurements

Los Alamos NATIONAL LABORATORY EST. 1943

OAK RIDGE National Laboratory

Qrypt entropy is based on a current and future innovation pipeline of quantum technologies, developed with research partners, including Oak Ridge National Laboratory and Los Alamos National Laboratory.

Entropy

Most randomization techniques employed for encryption keys today only have the appearance of randomness. Since they are typically generated using computational algorithms based on a short seed or a physical measurement, such as a resistor's thermal noise, they are inherently predictable. In fact, in the past few years, cybercriminals have created malware that has enabled them to defeat the so-called randomness of encryption used on government and enterprise networks.

Qrypt Quantum Entropy protects against such attacks by leveraging high-quality quantum sources to extract and deliver truly quantum random numbers. Plus, a roadmap of multiple quantum source types provides protection against failures of any single source type. Available for integration directly from the Qrypt Quantum Entropy API, random numbers are not re-used and can be supplied at rates required for production scale applications. You can address the risks from bad random numbers today, including from entropy starvation, as Qrypt is integrated into rngd providing entropy to /dev/random[2], and to Hashi Vault through Entropy augmentation.

Qrypt makes it easy for developers and SysOps teams to integrate intelligence-grade quantum security services into applications and infrastructure.

Key Generation

Qrypt Quantum Key Generation employs infrastructure consisting of high output quantum random number generation (QRNG) appliances distributed over multiple data centers to establish multiple pools of random numbers in the cloud. Client devices can then use local cryptographic extractors available in the Qrypt SDK to generate truly random and secure one-time pads and symmetric keys in a way that ensures no two pads or keys are ever the same. Plus, since the one-time pads and keys are never transmitted, they can't be intercepted.

Qrypt protects you against today's immediate and most sophisticated classic threats while future-proofing you against tomorrow's inevitable quantum threats and failed algorithms.

Secure Tunnel

Qrypt Secure Tunnel enables you to quantum-secure critical traffic with the use of one-time pad encryption. Think of it as a service that encrypts traffic before sending it over the network and decrypting the traffic on the other side – all using keys that have never been transmitted and an algorithm that is proven secure. For example, if you have a solution that stores and retrieves AES256 keys in a Hashicorp Vault, you can use Secure Tunnel to secure the transport of those keys by creating a one-time pad-encrypted tunnel. Since the data is quantum-secured with one-time pad encryption, even if the encrypted data is captured, the data is secure because the encryption can't be broken and the key was never transmitted and available to the attacker in any form.

Qrypt fortifies your quantum risk posture across all the stages of your NIST and NSM compliance transition.

You can also drop a Secure Tunnel container into or in front of any existing workflow, such as between your current hardware security module (HSM) and key clients to immediately and permanently quantum-secure transmissions. Secure Tunnel can also be deployed in your cloud environment to route critical traffic through it, and ensure your encryption keys remain quantum-secure. In these ways and others, Secure Tunnel can also become a powerful and flexible aspect of your secrets management workflows.

[1] Nicole Sganga, "Chinese hackers took trillions in intellectual property from about 30 multinational companies," CBS News, MAY 4, 2022, www.cbsnews.com/news/chinese-hackers-took-trillions-in-intellectual-property-from-about-30-multinational-companies/.
[2] https://github.com/nhorman/rng-tools

Qrypt for the federal government

As agencies transition to NIST requirements, Qrypt Quantum Security can quantum-secure long-term sensitive data now with perfect secrecy and permanent encryption.

Qrypt for QKD

Go beyond the limitations of QKD by completely eliminating key capture vulnerability in a viable, cost-efficient, and quantum-secure manner today.

Qrypt for financial services

Improve crypto-agility, PQC compliance, and go beyond the limitations of QKD. Stop transmitting encryption keys to reduce your risk today. And be quantum-secure for the future.

Qrypt for telco

For communications that matter the most, layer in quantum security over existing infrastructure now. Go beyond quantum-safe, be quantum-secure.

Qrypt for secrets management and key management

Improve security and simplify key exchanges. With Qrypt, you can easily drop-in and quantum-secure key exchanges or eliminate key transmission altogether.

Quantum Secure Encryption

Designed to outlast even the future's most powerful quantum computers, Quantum Secure Encryption protects data now and in the future while eliminating the high cost and effort required to replace tomorrow's failed cryptographic algorithms. With Qrypt Quantum Secure Encryption you encrypt your data once and the algorithm will never fail - even if PQC does.

Quantum Secure Encryption employs the properties of "perfect secrecy" and one-time pads, as defined in Claude Shannon's work. Since one-time pads provide encryption that's been mathematically proven to be unbreakable, they have become the gold standard for the most demanding environments, including within the intelligence community.

However, for many years the limiting risk factor for one-time pads had been the need to transmit keys, which until now has been the biggest encryption vulnerability shared by all encryption methodologies. Qrypt has pioneered a unique and efficient way to eliminate the need for key transmission. So, now Quantum Secure Encryption lets you use the power of one-time pads' perfect secrecy to give your data permanent protection.

Quantum Security SDK

The Qrypt SDK lets you deploy Qrypt Quantum Security in containers or part of a micro-architecture without additional hardware. It provides familiar developer tools based on modern development practices that let you easily integrate quantum-secure capabilities into your applications, hardware, and infrastructure without being an expert in cryptography. The SDK includes client library SDKs, cloud-based REST services, command-line clients, and guidance to help you integrate post-quantum security into your applications and services.

Available for download now.

Safeguard your data and communications with perfect secrecy.

Qrypt

Qrypt's mission is to protect the world's data. Ending encryption key transmission, the Qrypt Quantum Security Suite hardens security and future-proofs encryption against quantum attacks. Qrypt's unique technology independently generates one-time pads and symmetric keys at multiple endpoints, so you can eliminate key transmissions from critical workflows today. Qrypt's team of engineers, physicists, and cryptographers is committed to creating a new standard in security.

Visit Qrypt.com to learn more about how Qrypt Quantum Security can dramatically fortify and future-proof your data security.