Data at Rest

Overview

The Qrypt quantum secure data-at-rest solution uses one-time pad encryption to secure important files or valuable information, including executive communications, trade secrets, scientific formulas, and more. Now, you can keep your most important data safe from malicious attackers, even in the event of a security breach, or data harvesting.

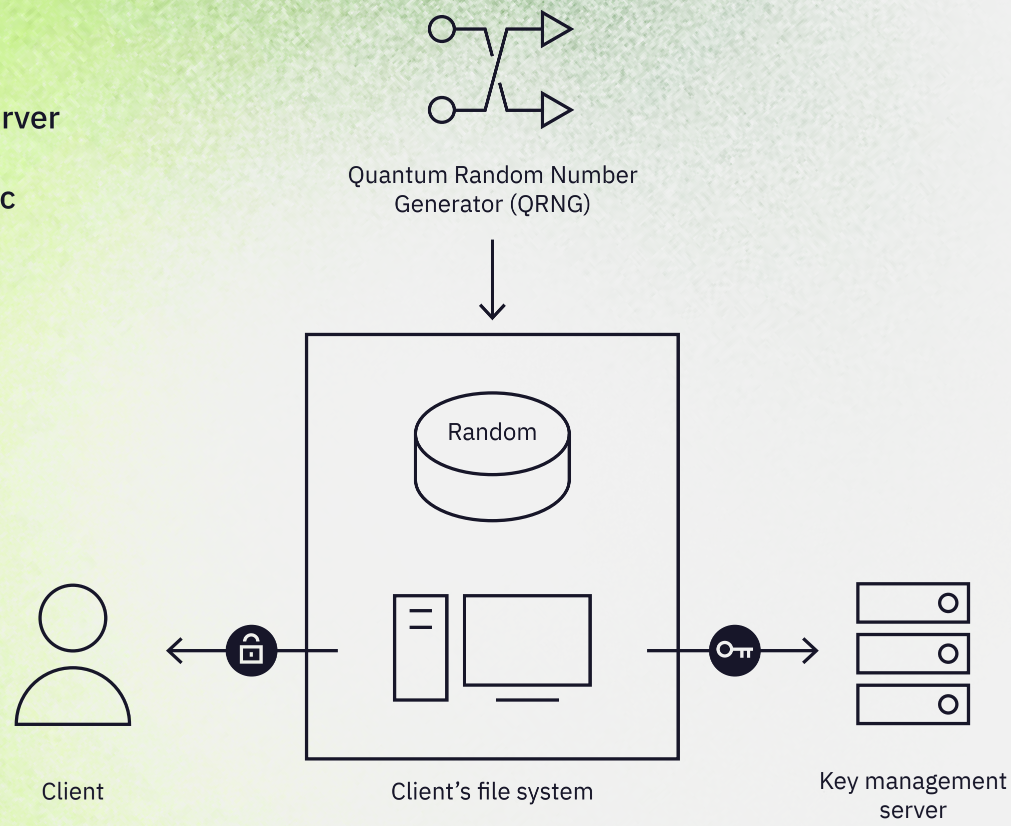
Our quantum secure data-at-rest product is powered by our patented BLAST algorithm, which leverages quantum random numbers from multiple sources of entropy to produce perfect one-time pads. Any user can quickly and easily encrypt sensitive files for distribution over untrusted public networks with no risk of compromise. As the shift to a permanent remote workforce continues, more data will need to be secured outside the physical enterprise.

Key benefits

- Underpinned by true quantum random
- Easily deployed with no hardware required
- Simply create a free account to get started

Use cases include:

- Large data sets, company server
- Large data sets, Azure/public cloud server
- Air gap systems



Because each one-time pad is quantum unique and bears no relation to the next, this approach to encryption is the only technique that cannot be “brute forced” by quantum computing. One-time pad encryption can only be broken if an attacker has access to the exact pool of random numbers used to encrypt the data, as well as the specific sampling and extraction parameters unique to that encryption session.

Qrypt

Getting started

Our cloud-based solution has an easy set up.

Go to **www.qrypt.com** to download our software to begin quantum secure encryption today!