## **₩**Qrypt

## Key Generation

## Key benefits

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

It is critical to ensure the data security of transmissions between locations, including financial transactions, intellectual property, or backup of sensitive data. Asymmetric public-key algorithms are a weak link for cryptography, as they are used to distribute encryption keys. The most common in use today, ECC and RSA, will be broken by future quantum computers and their replacements are also not guaranteed secure. There are now reports of hackers harvesting traffic to be decrypted later with a quantum computer. Qrypt Key Generation addresses this problem by independently generating identical encryption keys at multiple endpoints — they are never sent or distributed. Harvested data can't be decrypted, as it does not contain the encryption key.

Another shortcoming of today's encryption keys is that they are based on random numbers that aren't actually random, so that keys could be guessed when advanced techniques using machine learning are employed. The only way to generate secure keys is to base the random on a well-engineered quantum mechanical measurement, yielding a high quantum signal to classical noise ratio. Qrypt Key Generation locally extracts keys from quantum random numbers from the Qrypt Entropy service. Not only are the keys quantum, increasing their security, but the local extraction protocol ensures Qrypt doesn't know your keys.



Quantum Key Distribution (QKD) is an alternative approach which uses dedicated quantum links to distribute keys over short distances. This method comes with significant challenges including high cost, dedicated connections, short distances, and low data rates. Qrypt's solution has equivalent security to QKD, and can be used in cases where cost and performance must be considered, or where dedicated links are infeasible. Take advantage of Qrypt Key Generation for keys based on quantum entropy that are independently generated at each end point by visiting the Qrypt portal at portal.qrypt.com. You can register to access the API, download the Qrypt software development kit, and get started with sample code today.



## **Getting started**

Go to docs.qrypt.com for getting started guides, code samples, and to download the Qrypt software development kit.

Data sheet

Key Generation