Terra Quantum

Quantum Security

Our Approach to a Secure Future

Business White Paper

By Terra Quantum AG
terraquantum.swiss

February 2023

New Risks, New Opportunities

Terra Quantum pioneers a range of quantum technologies with the mission of leading the quantum revolution from meaningful solutions today to a more prosperous future tomorrow.

The development of quantum technologies will disrupt many industries, creating new opportunities and at the same time, new risks.

Currently, there is considerable concern about the nefarious use of quantum technologies for illegal hacking. It is expected that in the near future, quantum computers will develop to such a point that they pose a significant threat to our current information security protocols, allowing hackers access to sensitive information globally by brute-forcing security problems previously uncrackable by classical computers. While companies in the financial and healthcare spaces are especially concerned with protecting confidential and sensitive information, all industries are aware of the financial losses and reputational damages that result from data breaches and should be proactive in addressing this threat.

This business white paper discusses the nature of the coming threat and details our comprehensive offerings and solutions for secure communication in the quantum age. These include Terra Quantum's novel Quantum Key Distribution (QKD) protocol, Quantum Random Number Generators (QRNGs) and Post-Quantum Library.

Modern Communication and The Quantum Threat

The Cyber Security industry finds itself in a never-ending arms race against ever more sophisticated and ingenious attackers, hacking groups and malicious actors. Companies today face myriad threats that exploit all kinds of vulnerabilities in their enterprises. The surface area of potential compromise is expanding, stretching from an organization's employees — who are frequently the target of phishing and social engineering attacks — to the supporting technological infrastructure that is all too often the subject of devastating evolving attacks and zero-day threats. This constantly changing threat landscape, organizations must be increasingly vigilant and proactive in preventing catastrophic damages to their business.

However, amidst all this chaos, one threat that is currently largely unaddressed looms large on the horizon. As will be explained in the section on the **"store now — decrypt later"** risk, for some data and some companies, it is already too late to prevent against it. This vulnerability exists in just about every network and internet service used across the globe.

> **Acting now may protect you from serious data breaches in the future.**
>
> *— Terra Quantum*

Quantum computers have the potential to help humankind overcome various technological limitations and solve our greatest challenges in both business and society. Their development is a double-edged sword because they will be able to run an algorithm capable of decrypting much of the world's confidential data. For further details, please see the technical deep dive section on quantum decryption. In short, any information encrypted using certain encryption methods (e.g., the RSA method) could be decrypted by a quantum computer. Currently, the enormous amount of information that is transferred using this kind of quantum-vulnerable encryption includes — but is not limited to — **email, direct messages, file transfers, financial information, internet browsing** and so on.

The "Store Now – Decrypt Later" Risk

Y2Q (also known as Q-Day) is the date when quantum computers will have advanced to the point where they can easily crack some of the public-key cryptography schemes that are used in communications everywhere from internet browsing to email messaging. Past this date, any individuals or organizations in possession of a quantum computer will be able to decrypt the information they have acquired that was secured with the quantum-vulnerable methods (e.g., RSA encryption).

Notably, this includes sensitive information that could be acquired today and might still be sensitive in the future. This is known as the "store now — decrypt later" threat. Because malicious actors can obtain copies of recently encrypted data and then wait until sufficient quantum computing resources have become available to decrypt and access the sensitive information, one could say that some encrypted data that exist today are effectively already stolen. This is best described by Mosca's theorem (See Figure 1. Mosca's Theorem).

Even though a portion of the encrypted data that exist today will become less sensitive and important with time, this is certainly not true of all data. Much of the most sensitive and private data types have very long shelf lives and though estimates of when Y2Q will arrive vary, some groups state that any sensitive data stored today with a shelf life longer than five to ten years is already at risk. From medical records within healthcare to bank details and transfer information, this threat is widespread across multiple industries.

NATO, the U.S. Government and a wide array of global organizations have already begun preparation for Y2Q, as it is understood that if swift action is not taken, the security of a vast proportion of global data will be compromised. As each day passes, organizations that do not address the incoming threat are increasing the risk of having their sensitive data stolen in the future.

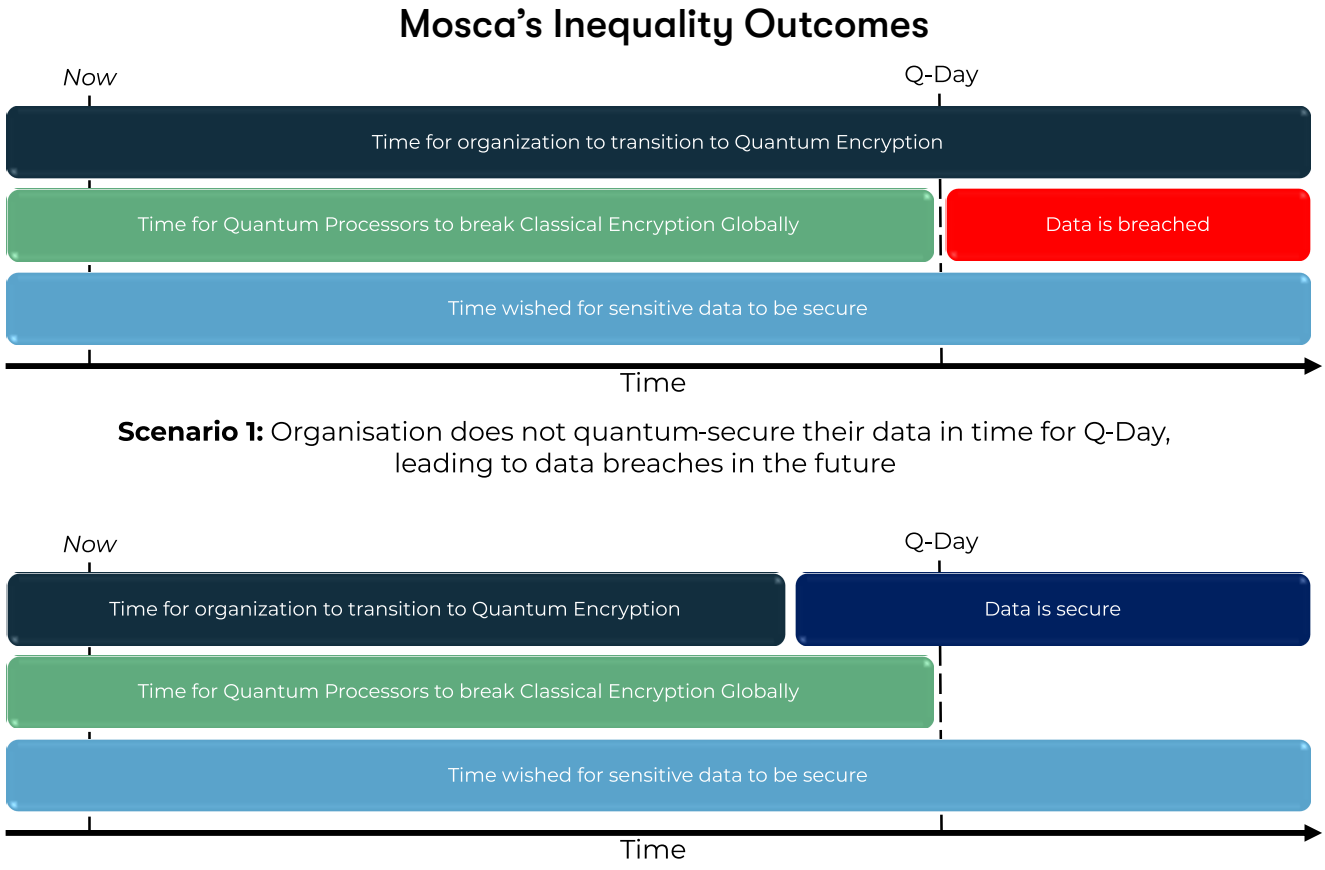


Figure 1. Mosca's Theorem

Technical Deep Dive on Quantum Decryption

The basis for all classical public-key encryption methods in use is the computational difficulty of solving certain mathematical problems. An example of this is RSA encryption, which is predicated on the problem of factorizing large integers into constituent primes — for which currently there exists no efficient algorithmic solution. These problems are called 'intractable' — there is no efficient algorithm to solve them. Therefore, these methods of encryption are secure simply due to the staggering amount of time it would take any classical computer — however large — to decrypt them.

However, this is not true of quantum computers. Quantum computers, and the algorithms that can be run on them, turn certain classically intractable problems into tractable ones. Which is to say, they become solvable in much smaller amounts of time and do not require exponentially more time for larger problem instances.

For instance, one such algorithm which enables this is Shor's algorithm, which allows quantum computers to tractably factorize large prime numbers, as well as to efficiently solve the so-called discrete logarithm problem. The algorithm shrinks the computational time to solve these problems exponentially. This means all the widely popular encryption key protocols based off these problems — such as RSA, Diffie-Hellman and Elliptic Curve schemes — will soon no longer be secure.

When quantum computers and resources become more widely available past Y2Q, malicious actors or organizations will be able to utilize them with algorithms such as Shor's to decrypt commonly used public key encryption protocols with relative ease. They will then have full access to sensitive data that should have been kept confidential.

Terra Quantum Provides Security as a Service

By exploiting the physics of the smallest levels of reality — quantum mechanics — as well as mathematics and computer science, we at Terra Quantum have developed quantum-secure technologies and protocols. They comply with the European Telecommunications Standards Institute (ETSI) and International Telecommunications Union (ITU) standards and will ensure confidential and sensitive data remains protected in the coming quantum age and beyond.

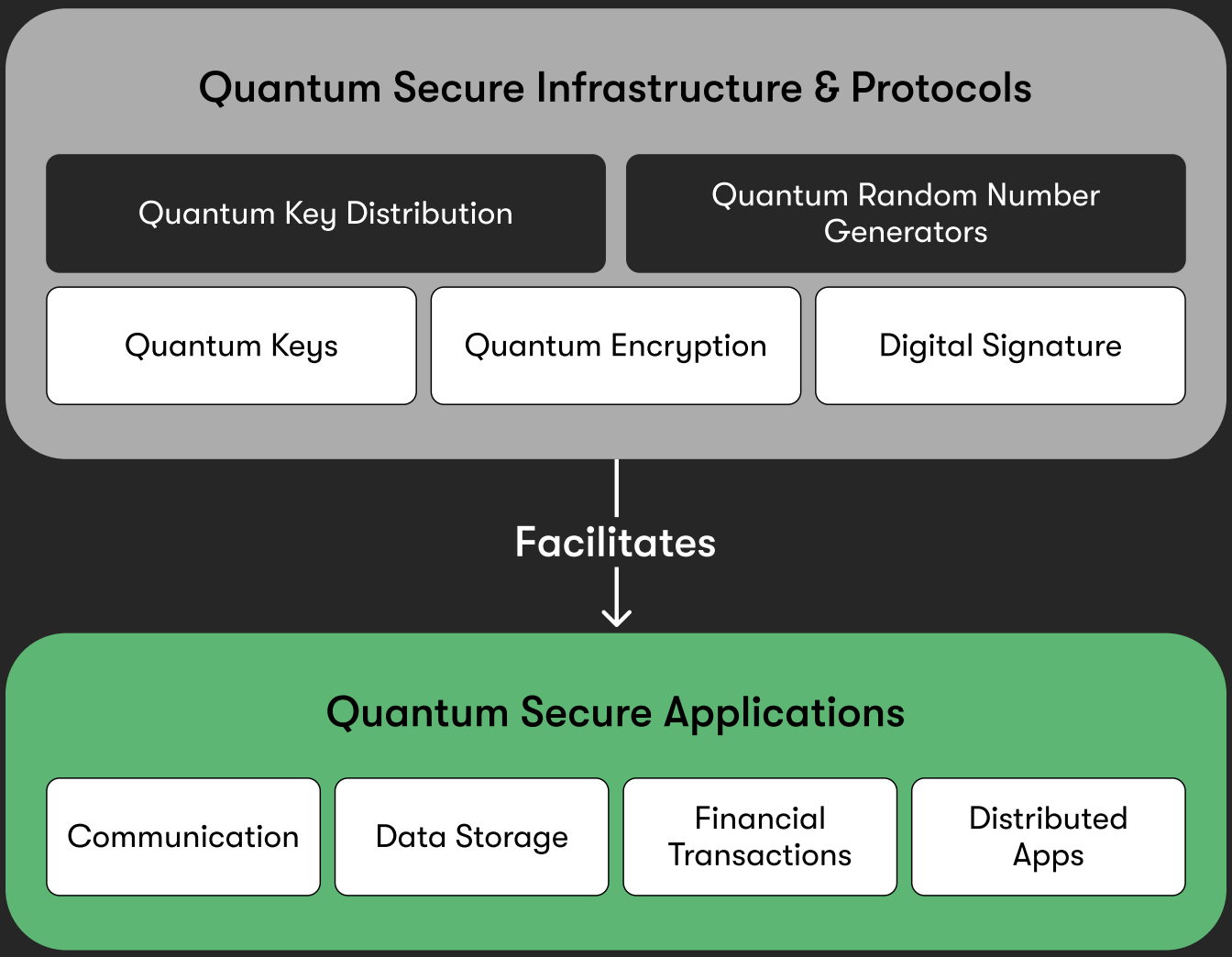
Terra Quantum can provide a complete end-to-end quantum upgrade to any network to facilitate secure communications in the quantum age. Our offerings form a comprehensive and secure total security approach.

Its foundations consist of three innovations:

- A Novel Quantum Key Distribution (QKD) Protocol
- Quantum Random Number Generators (QRNGs)
- A Post-Quantum Library

It would take today's classical algorithms roughly $8.5x10^{590}$ years to decrypt the RSA 2048 bit public key encryption protocol.

A quantum computer with 4099 fault-tolerant qubits could achieve the same outcome in just ten seconds. Some publicly available roadmaps show this number of qubits will be available by 2025.

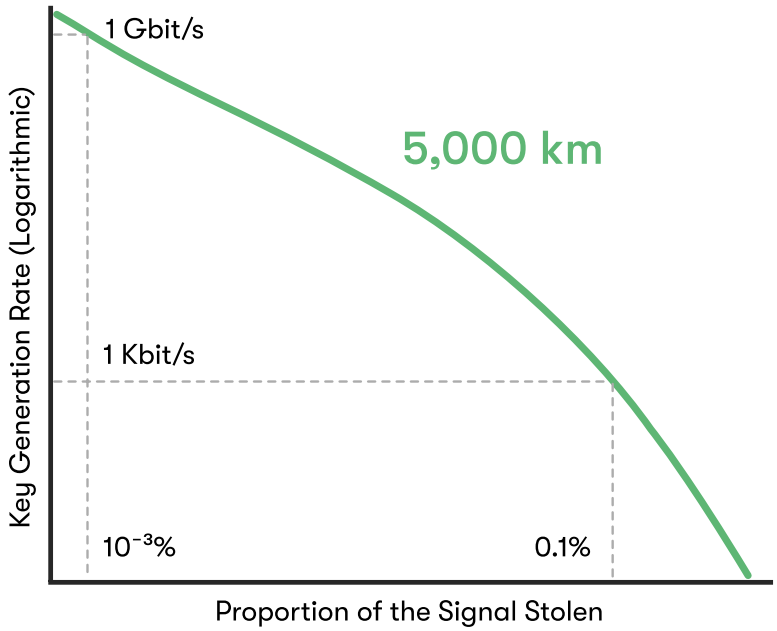


QKD and QRNG enable and facilitate quantum secure infrastructure, which is founded for future quantum secure applications

Figure 2. Terra Quantum's Integrated Security Approach

Our Novel Quantum Key Distribution Protocol

The goal of quantum key distribution is to create an authenticated, confidential channel. Prior approaches to achieving this have only succeeded in a very limited way but Terra Quantum's patented set-up enables secure communication at a much higher bit rate and between users that are considerably further apart.



40,000 km
Transmission Distances

1 Gbit/s
Key Generation Rates

0.001%
Leakage Detection Precision

Figure 3. Our QKD protocol performance

For all QKD schemes, there is a trade-off between the transmission distance and the key generation rate. Our solution is compatible with standard telecommunication fibers and yet it allows high-speed communication over global distances. For further information on this technology, please see the technical deep dive section.

Technical Deep Dive on the QKD Protocol

The goal of QKD is for two parties to obtain a shared sequence of random bits, known only to them, that they can then use for secure communication through an ordinary classical channel. Typically, these users are referred to as Alice and Bob and at the start of any protocol they have a classical channel that is:

- Authenticated, meaning that Alice and Bob know they are talking to one another and that their messages cannot be changed

- Completely public, in the sense that any eavesdroppers can listen in

Between Alice and Bob, there is also a standard optical fiber through which photons encoding quantum information can be sent (though it should be noted that the classical channel can pass through this physical cable as well, resulting in a single physical connection that hosts two channels). In conventional protocols, this quantum channel is completely at the mercy of an eavesdropper, commonly known as Eve. In the Terra Quantum scheme, Alice and Bob can now monitor the characteristics of the quantum channel and detect any manipulation of the light signal by Eve. This enhanced ability to detect eavesdropping allows the Terra Quantum approach to achieve unprecedented performance.

Experimental Considerations

Due to the high signal losses that occur as transmission distances increase, traditional QKD protocols face severe hardware limitations. The only ways the users of these protocols can go beyond small-scale implementations is to either wait until quantum repeaters become technologically mature or they must put their trust in intermediaries who could act maliciously. Terra Quantum have developed hardware that can repeat light signals by means of optical amplification. Our innovative bidirectional optical amplifiers serve as extremely reliable repeaters, which do not have to be trusted.

Theoretical Considerations

In the Terra Quantum protocol, Alice and Bob can distinguish between signal leakages that are caused by Eve and natural losses of the signal that we know (from the second law of thermodynamics) cannot be exploited by Eve. As a result of this, Alice and Bob can alter the signal so that Eve's measurements are so plagued by Poissonian statistics that she cannot tell ones apart from zeroes, yet Bob, who can be extremely far away, receives clear, high intensity signals.

Quantum Random Number Generators

In information security, random number generators (RNGs) generate the session keys that are used to encrypt and decrypt all the information transferred during one communication session. Randomness is crucial to this process because if a malicious actor were able to predict the behaviour of an RNG, it would render the encryption completely ineffective.

For many industries, security is a priority. Cloud services are an interesting case. As security functionalities move to the cloud, the local source of randomness that was previously used may accidentally be replaced with a weaker source. Since cloud providers handle a huge volume of data in motion, there is a strong need for access to QRNGs.

The financial industry is another noteworthy sector. In addition to their clear need for high security levels, random numbers are essential to how they optimize their portfolios and stress-test their risk levels. Consequently, QRNGs would enhance several of their most crucial business operations.

At Terra Quantum, we have developed quantum random number generators (QRNGs) that leverage the principles of quantum physics to create fundamentally random and unpredictable session keys. Our devices use single-photon emitters and detectors to generate keys. These have passed industry-standard randomness tests, such as NIST 800-22 and DieHard. See the technical deep dive section on QRNGs for further details.

The Terra Quantum QRNGs can be used to generate session keys in conjunction with either existing cryptographic protocols or our novel QKD protocol. To handle these options, we have developed a post-quantum library.

Figure 4. Terra Quantum's Single Photon QRNG

Technical Deep Dive on QRNGs

Random numbers can be generated algorithmically, with specialized software, or physically, with specialized hardware. The numbers produced by software RNGs are called pseudorandom because while they appear random, a clever analysis of the underlying algorithms could reveal a pattern.

Hardware RNGs, on the other hand, make use of a physical process to create entropy. Whether this process is described by classical physics, which is deterministic, or quantum physics, which is probabilistic, is extremely important. In the classical case, careful investigations may uncover regularities in the sequence of numbers but according to our best theories, this is completely impossible for quantum processes.

To make this clearer, the classical action of flipping a coin is not as random as it seems. Turn on a slow-motion camera for just a second, run the observations through a physics simulation package and you can deduce the outcome extremely reliably. In contrast, there are no hidden variables in quantum systems that would allow anything similar to be done. In fact, the recent 2022 Nobel Prize for Physics was awarded to physicists who showed this experimentally.

At a high level, our photonic QRNG works in the following, as described in Figure 5. A single photon is emitted by light source (LD) and travels towards the beam-splitter (BS), where it is put into a quantum mechanical state known as a superposition. Measurement of the photon by one of the single photon detectors (SPDs) then reveals whether the photon was reflected and travelled down path R or was transmitted and travelled down path T. The two outcomes occur randomly and so by assigning a zero bit to one of the outcomes and a one bit to the other, we obtain a truly random sequence of bits.

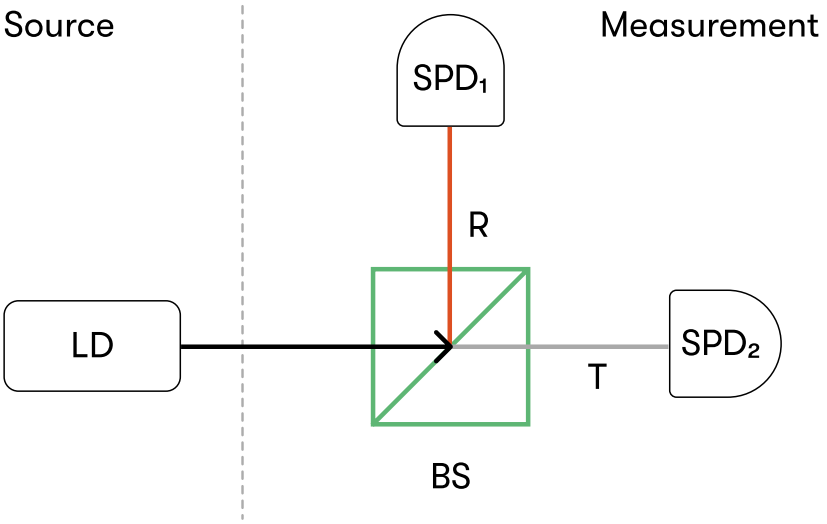


Figure 5. Example Quantum Beam Splitter RNG Design

Post-Quantum Library

The transition from conventional cryptographic set-ups to ones that incorporate QRNGs and QKD will require solving various practical problems. Many of these are dealt with on a single-session basis with our QKD protocol. However, the challenge remains to find a way of incorporating these protocols seamlessly into existing systems and platforms.

Currently, there are several classical standards for storing keys. Unfortunately, they are not adapted for instant users and the volume of the stored key information is limited, as is the type of stored keys. This could lead to the users' security levels being reduced if they cannot obtain a high-quality key far from the source of the key.

To solve this, Terra Quantum have developed a post-quantum library designed to supply random numbers and quantum keys in any communication network, regardless of the hardware platform, network architecture, encryption equipment or software used. This one library has a broad range of features that cover all applications and use cases.

Our library — which is levels above any alternative — adheres to all the relevant standards. Every fine detail and nuance have been thoroughly considered so that (a) the security is as strong as possible and (b) programmers will find it easy to integrate into their applications. The following section on our key container serves as a useful, illustrative example.

Key Container for Symmetric Keys and Post Quantum Keys

The main difference between a post-quantum container and a classical one is that it must contain keys of a different format and in large quantities. It should also allow the quantum keys to be changed remotely without direct access to the QKD.

Therefore, we have developed a key container that contains a large set of electronic signature keys as well as special keys that allow a user to receive new electronic signature keys remotely on the QKD or QRNG.

All these changes will enable methods to distribute private keys that will be quantum stable. This will keep the Internet and its security in the form we are used to, without a complete overhaul.

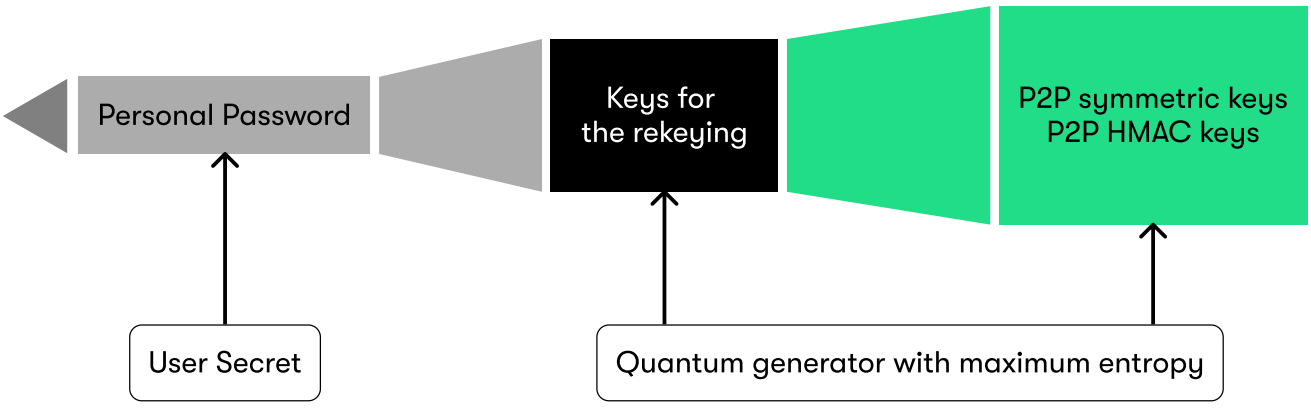


Figure 6. Fortifying Passwords with Quantum Generators

Roadmap to Quantum Security

These quantum security foundations form the basis of a wide variety of quantum-secure applications, including:

- Quantum-secure VPNs for secure internal- and B2B-communication networks
- Peer-to-peer (P2P) communication apps for video calls and messaging
- IoT device security (any device to any device) – including sensitive location data (e.g., between a car and a satellite) and personal health data
- Secure corporate-to-customer communications – with applications ranging from the financial to healthcare industries

We can also enable practical implementation of alternative QKD protocols, along with a Private Quantum Cloud (PQC) for those seeking a basic level of quantum cloud security. We can provide a modular approach to any of these implementations or enable an entire end-to-end security upgrade.

How to Quantum-Secure Your Organization

1. Organizations are advised to conduct a thorough inventory to determine what systems and processes use public-key cryptography. Clarity should be obtained on how the cryptography is used to protect the confidentiality and integrity of data at rest, data in use and data in motion. This applies to numerous types of data, including financial, legal and industry specific.

2. Organizations are advised to assess what quantum-secure technology upgrades are appropriate, while seeking to discover any technical constraints that their systems may have with regards to implementing security upgrades.

3. Organizations should also work with service providers, partners and customers to coordinate their adoption of any quantum-secure technologies, such as to preserve the interoperability of their existing infrastructure and to ensure there are no service disruptions in the process of securing data.

4. Organizations can contact Terra Quantum to execute the decided implementations of quantum-secure technologies.

5. Overall, as we approach Q-day and beyond, organizations should seek to adopt a long-term, quantum-agile strategy when it comes to their security upgrades.

The Time to Protect Ourselves is Now

Due to the threat of data being stored today and decrypted later, now is the time to act to quantum-secure your organization. The quantum age is coming and organizations must be proactive to not only secure benefits but protect from their threats.

Terra Quantum are leaders in providing security as a service: our Quantum Key Distribution solution allows keys to be sent long distances and with a high bit rate; our Quantum Random Number Generator solution produces truly random numbers; and our Post Quantum Library is easy for coders to use for an extremely wide range of applications.

Quantum is now. Quantum-secure your network today.

Get in Touch

Website:
https://terraquantum.swiss/

Email:
info@terraquantum.ch

Address:
Kornhausstrasse 25
9000 St. Gallen, Switzerland

Phone:
+41 71 444 0000