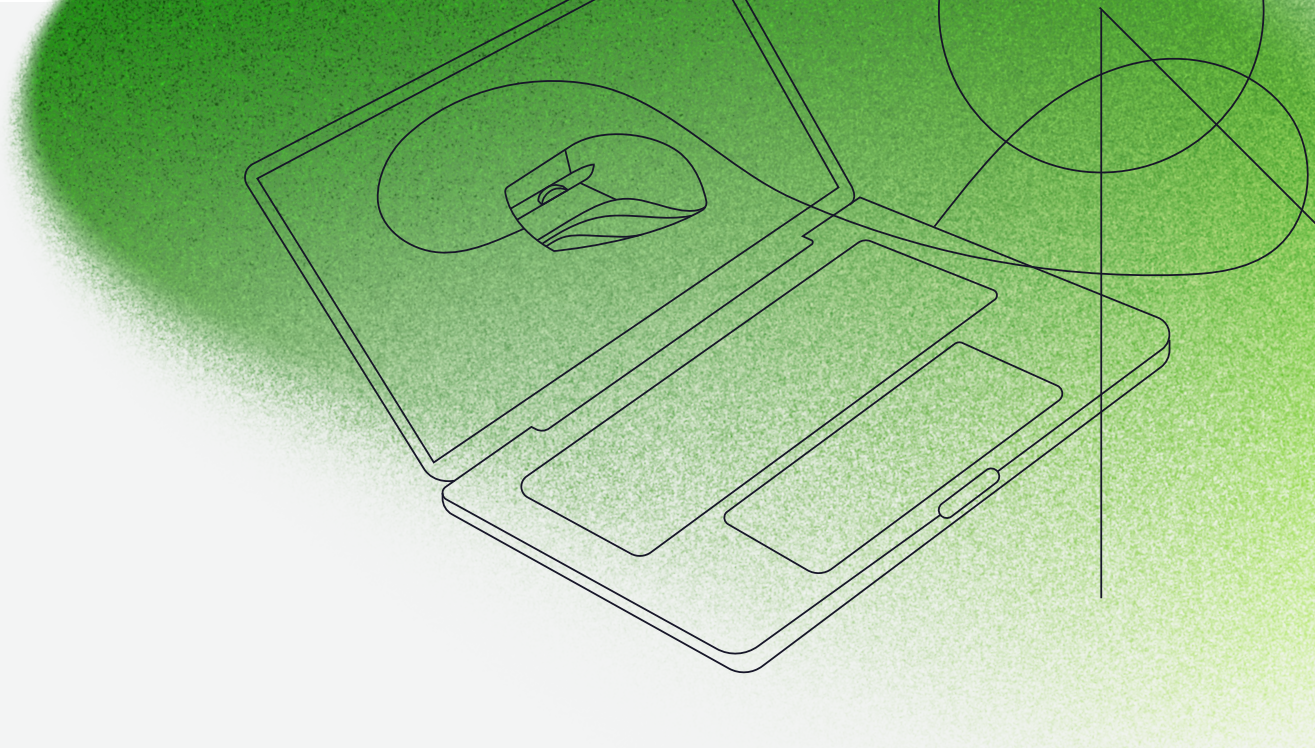




Everlasting Security

Quantum Secure Solutions from Qrypt



Introduction

The emergence of quantum computing will be marked by many milestones, both scientific and with practical significance to business. One notable milestone includes rendering current asymmetric encryption schemes obsolete, but there will be many before it. The scientific community has explored the implications of quantum information science and how these concepts may be applied to computing for over four decades. In 2016, the first quantum computers were made available on the cloud, though their use was limited to scientific and educational purposes given their small size. Since then, the scale of these systems has grown so that they can no longer be simulated by classical computers, however they continue to be for research and development rather than for productive business value. This decade, many have predicted that applications will emerge where quantum computing is able to demonstrate an advantage over classical computing. First there will be advantage for very narrow use cases with many constraints. Over time advantage will expand to more general use as the quantum systems improve and the applications research progresses. However, this expansion will not be linear, businesses will see a series of moments where value is unlocked over the coming decades.

One of the technological advancements will be the emergence of universal fault tolerant quantum computing, which will allow numbers to be factored efficiently – which a classical computer cannot do. Once a quantum computer can factor numbers of sufficient size, encrypted data based on RSA will be at risk as it can be decrypted. Other asymmetric algorithms are also at risk, from similar threats based on quantum computing.

Another threat vector for encryption is the attack on the random numbers used as seeds for the generation of cryptographic keys. If an attacker can predict how the random number generator will behave, then they can reduce the amount of time it will take for a brute force attack of the encryption – ultimately compromising data security. Here quantum can be the solution rather than the threat. Instead of leveraging quantum mechanics for compute, it can be leveraged to improve the random seeds so that they cannot be predicted. The increasing capabilities of machine learning improve their ability to characterize non-quantum sources of random, in an environment where the attack surface is growing due to increasing volumes of sensitive data.

The following overview provides insight into Qrypt's suite of solutions preparing organizations for threats in the age of quantum computing. A solution can only be deemed secure if it addresses both the threat of attacks on random and the future threat of a quantum computer decrypting data stored today. Both threats outlined are relevant today and being actively targeted. Attackers will copy encrypted data today, and hold it for future exploitation, while victims remain unaware.

What is Random?

In science, random is an unpredictable pattern or event for which the outcome cannot be known in advance. While rolling dice or flipping a coin may appear random and unbiased, they are not at a fundamental level. Knowing the initial speed, angle and other parameters always predetermines the result. Robots are good at controlling these details and can perfectly flip heads every time, proving there is nothing inherently random about it. This can be done in principle for every classical physical system governed by the basic laws of physics, even when we don't have an intuitive understanding of how.

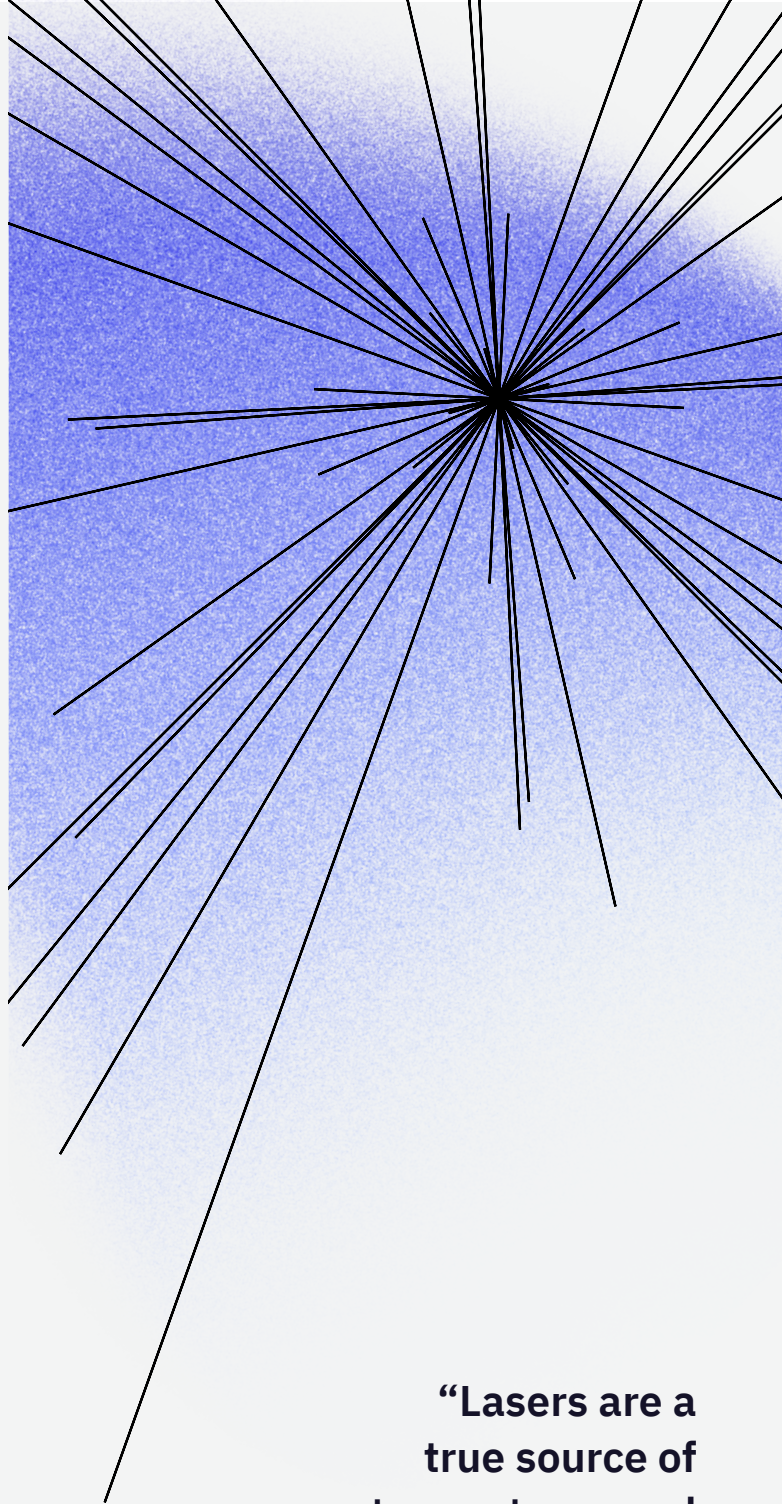
However, at the scale of the very small, very cold, and other extreme environments, classical physics can't describe how these systems behave, and quantum mechanics steps forward. The outcome of a quantum measurement is unknowable no matter the amount of information we have beforehand, even when the state prior to measurement is perfectly known. It's like rolling "quantum dice", where the output really is random. In contrast to the classical world of everyday experience which appears deterministic, measuring a quantum system changes it, and the outcome of such a measurement is probabilistic. As such, only quantum measurements are truly random. Although everything in the universe is made of particles that behave quantumly and is the sum of

quantum events, when many of them are combined into a large system, like tossing a coin, the quantum effects are overwhelmed by classical effects and become invisible. The quantum contribution to the randomness is still there, but unobservable. The coin flipper's actions determine heads or tails, not quantum uncertainty.

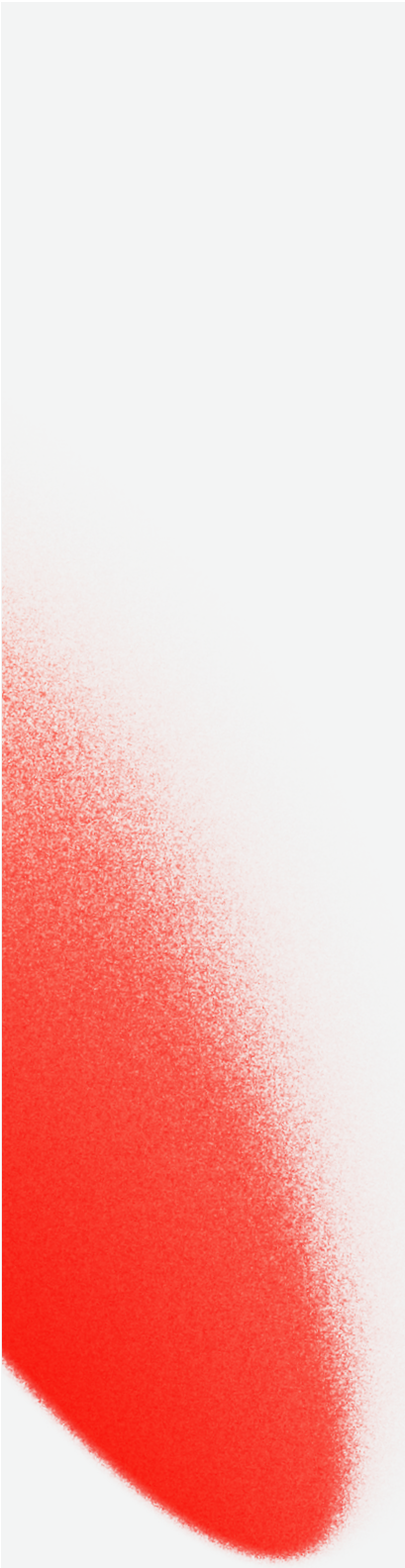
The Importance of Random

Any institution that needs to ensure security, must consider the random numbers and random number generators used to create them as a part of their overall security strategy. Perhaps the most widespread application of random numbers is in cryptography, which secures our data and communications. Random Number Generators (RNGs) are used to create the keys for locking emails, websites, text messages, and HTTPS connections in browsers. The keys are created based on a random number called a seed. If these seeds are not actually random, then an attacker may guess the keys used to encrypt messages. Therefore, the entire basis for security is directly correlated with the ability to create truly random seeds.

While exploiting weak random may seem improbable, it is practical and is currently an active threat in use today. Cryptocurrencies rely on randomness to secure their virtualized value in blockchains and digital wallets. An e-banquit was able to guess Ethereum's private keys, and used them to permanently transfer millions in Ether (e-coins) to themselves. Similar unknown thieves stole millions in Bitcoin. With 115 quattuorvigintillion possible keys (2^{256}), it is impossible to predict a single key with



“Lasers are a true source of quantum entropy and may be carefully configured to produce a very fast stream of random digits.



all the computing power on Earth. The odds of guessing a single key are much worse than winning the Powerball lottery multiple times in a row. While these cases appear to have been isolated, examples of attacking RNGs and the software mechanisms for creating keys has become more widespread and devastating. In 2019, Reductor malware was discovered installed on many internet browsers. It caused the pseudorandom number generation used to make keys for HTTPS connections to become predictable in a way only known to the attackers. This allowed them to passively decrypt any transaction or message used by the compromised browsers without triggering suspicion typical of an active attack. FIPS-certified Yubikey tokens used to authenticate to government networks suffered from flawed randomness again resulting in a predictable number of bits being identical. FIPS products go through rigorous independent lab testing and evaluation before use on government systems, which implies the randomness problem is far more pervasive and demonstrates that randomness cannot be proven with a certification. Dual_EC_DRBG is apparently a deliberate intelligence community attempt to compromise a ubiquitous, standards-based RNG in 2006. Although this possible kleptographic backdoor was quickly questioned by researchers and later deprecated, it was deployed on large Juniper Networks infrastructure systems around the world and discovered in use as late as 2015.

All of this evidence demonstrates that random number generation is an important element that needs to be addressed in any holistic security strategy. Existing approaches to random number generation are insufficient given modern security requirements in the face of the sophisticated attack methods.

Entropy and the Sources of Random

Although many natural phenomena appear random, they can often be modeled to reveal their patterns, and are therefore inappropriate sources of unpredictable random numbers. The term entropy is often described as a measure of the disorder in a system, and has a formal physical definition in science. For example, popping a small helium balloon will evolve a highly ordered state (all the gas in a small space) to a high entropy or disordered state as the helium diffuses through the air in the room. Helium is lighter than air and will tend to fill the space closest to the ceiling, displacing the air, at a predictable rate. Numbers extracted from this experiment can appear unpredictable, but they are not. Popping a helium balloon may sound esoteric in a discussion about the

applicability of random numbers for security, however other systems that can also be modeled are being used as sources of random numbers today. So called True Random Number Generators are based on physical measurements that are converted to random numbers. Thermal noise is an example of a physical process that is being measured in these systems to generate random numbers, however as this is a physical system that obeys deterministic laws it is a physical system that can also be modeled. Practically speaking this is difficult for humans, however with advanced techniques in machine learning characterizing these random noise sources is within reach. These predictable systems are unsuitable for producing random numbers where verifiable sources are required, which are essential for cryptography.

Good sources for truly quantum random measurements must be quantum effects that can be isolated and measured with high fidelity compared to other classical effects that may influence the measurement. The presence of a quantum effect doesn't mean that there is a quantum measurement that can be isolated from other classical effects. Quantum tunneling is an example of a quantum effect, however a measurement such as a leakage current through an insulator is influenced by many classical effects as well. It must be possible to isolate and measure the quantum effect, to take advantage of the benefits of quantum randomness.

Quantum sources must also be practical for systems integration and support sufficiently high data rates. Possible quantum measurements include emissions from radioactive decay, the phase of laser pulses, cosmic rays from outer space, and many others. While radioactive decay is an excellent source of quantum entropy, it is unsuitable for installation inside a computer or cell phone. Fortunately, fiber optic infrastructure and similar systems use lasers and detectors which are quantum in nature, and already operate at the speeds required for security use cases. Lasers are a true source of quantum entropy and may be carefully configured to produce a very fast stream of random digits. However, the process is very easy to get wrong and can result in output that only appears random. The engineering of these quantum random number generators (QRNGs) must exclude all the sources of classical noise to purify the quantum signal, otherwise, they are no better than non-quantum hardware and their predictability may be discovered once already deployed. Other types of quantum sources use qubits and more sensitive electronics like SPAD arrays, which are capable of detecting a single particle of light (a photon). Any quantum entangled system can produce a truly unpredictable set of outcomes that can be converted into a series of random digits suitable for cryptography.

High rate QRNGs based on high fidelity measurements of quantum effects must become the standard for encryption because they have measurable and well-studied randomness.

Their true value is in the physics guarantees of inimitability. For example, there is no conceivable predictability if used to make encryption keys, which could otherwise result in users inadvertently using identical keys. This is more than a hypothetical concern. In the case of digital certificates, a 2019 study discovered in a sample of 75 million RSA certificates used on the internet, 1 in 172 share a common factor, a stunning security flaw, and an unambiguous indicator of almost no entropy at all. The implications are far reaching, including that the possibility of compromise is again within reach of attackers, as the computational protection of the underlying algorithm is no longer valid.

Qrypt Entropy-as-a-Service

Qrypt has built the first generation of Entropy-as-a-Service using cloud infrastructure, which makes QRNGs available to any internet-connected device. As more devices get securely connected via the internet and begin using stronger algorithms, the need for random numbers grows at an unsustainable rate for modern computing systems — they were designed to calculate with precision, not to produce disorder essential for randomness. IoT and always-on 5G networks are always tethered to cloud as-a-service products. The Qrypt service produces gigabits of random every second and can scale on-demand to meet high data throughput requirements. Qrypt has multiple entropy sources which are continuously checked for the healthy operation of their physics instrumentation and statistical analysis of the bits they output. Different types of physical quantum processes are used in an orthogonal configuration to prevent side-channel attacks from compromising their operation and causing them to yield nonrandom. The independent quantum random bit streams are then combined prior to being sent to a user.

When the Qrypt SDK is used, additional mathematical functions are performed at the client end-point to mix the raw random received from the Qrypt Entropy service, which precludes Qrypt from having any knowledge of its final state in use. This last step preserves the pure quantumness of the random and obfuscates its final application utility from the cloud, while also ensuring its uniqueness.

Examples of Use Cases

Domain	Use Case
Public key infrastructure (PKI)	<ul style="list-style-type: none">• Root of trust• Key generation• Key management
Digital signatures	<ul style="list-style-type: none">• Contracts• Secure email• Time stamps• Logs
Blockchain	<ul style="list-style-type: none">• Contracts• Asset provenance• Proof of work
Data security	<ul style="list-style-type: none">• Network security and protocols• Database encryption• Data at rest encryption• Zero trust

Post Quantum Cryptography from Qrypt

NIST is sponsoring a global competition to standardize a new suite of quantum resistant algorithms, because quantum computers will likely defeat the asymmetric algorithms used for encryption of most internet transactions. Post quantum cryptography (PQC) refers to cryptography that is implemented using these algorithms that are thought safe from quantum attack. When combined with existing symmetric algorithms like AES, the combination forms a PQC solution for an online transaction.

Migration to PQC algorithms will take time, and it is important that the process is started so that the transition is fully completed prior to the arrival of capable quantum computers. Any encrypted transfers that are initiated with RSA, ECC, or other popular public key algorithms or protocols will no longer be safe. However, the implications aren't limited to only the time period when the quantum computers are able to do the decryption.

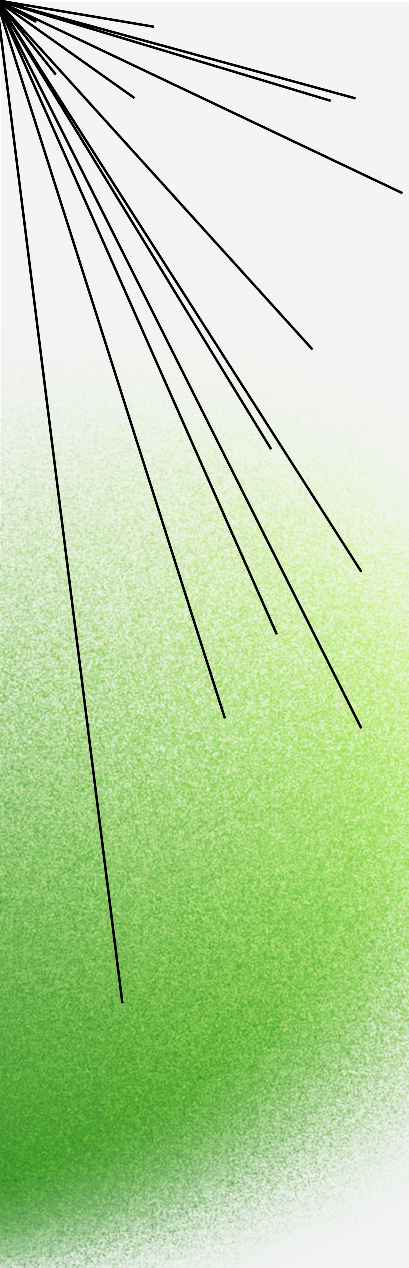
An attacker that steals data today, encrypted with today's encryption, will be able to decrypt it later with a quantum computer. Migrating to PQC algorithms does not fully eliminate this threat, as it is not proven that the PQC algorithms are quantum-safe. Without a proof of security, we are relying on study and scrutiny to identify and evaluate potential weaknesses – this is the purpose of the NIST competition. However, given the limited time available to set this standard, and the novelty of the PQC algorithms there is not a high degree of confidence that one or many of them will not be compromised in the future. If an attacker had stored data encrypted with a PQC algorithm that was later compromised, then they will be able to decrypt it.

Any security solution needs to evaluate all of these possible threats, and design the cryptographic system that uses these algorithms with them in mind.

BLAST

There are two classes of cryptographic solutions, one is secure against all conceivable computers that could ever be built, even in theory, quantum or otherwise, and the other is unconditionally secure against any advances in science. The latter has the property of “everlasting security”, which simply means it cannot be broken even in principle. In 1947, the basis for these protocols was proven by Claude Shannon and are known as one-time pad (OTP) systems. To use an OTP, two copies of the same OTP encryption key must exist at the sender's and receiver's locations. Practically speaking, this means that your security ends up being limited by the mechanism that you are using to distribute the OTP.

Governments often use OTP encryption, however typical implementations are costly and require courier delivery of the key material to solve the distribution problem, which is impractical in modern information systems. Quantum key distribution (QKD) networks



can also be used to distribute this key material securely, as it relies on quantum mechanics to ensure there is no eavesdropping. However, QKD requires dedicated fiber infrastructure, is costly, and is constrained in transmission distance. Ultimately, each of these distribution solutions has drawbacks that make them impractical for broad use.

BLAST is an architecture pioneered by Qrypt that solves the distribution problem by eliminating the need for distribution – instead identical keys can be securely generated at multiple endpoints. The protocol leverages cloud infrastructure, QRNGs, and PQC technologies, ensuring that the solution not only addresses the threats of quantum computers but also the threats of poor random. This hybrid approach relies on a network of high output QRNG devices distributed over multiple data centers, which establishes a large effective pool of random numbers accessible by authenticated users. Individual clients are allowed to sample and download only small portions of the available random from this constellation of servers, followed by the application of local cryptographic extractors which generates the keys directly on the client device. The key can be a standard AES key that can be subsequently used for symmetric encryption, or an OTP enabling a provably secure solution. The final extraction step obfuscates OTP creation from the servers providing the pool of random, which means that Qrypt cannot reproduce the AES or OTP keys generated. Extractors preserve the quantumness of the entropy used, ensuring no two OTPs or keys are ever alike.

BLAST can be applied to key generation in this manner, to allow for generation of identical keys by several parties. The difference is the sampled random from cloud QRNG appliances must be synchronized across all parties communicating instead of from a local pool. This can be achieved asynchronously when users are not online at the same time, as in messaging apps. Client devices must sample random from the same pools of random in the cloud, followed by local extraction to reach AES or OTP agreement. The cloud pools of random are overwritten with fresh quantum random and never used again, when certain conditions are triggered – for instance time based or when a percentage of the pool is consumed. Only a small fraction of this repository is accessible by any user and only a fraction is ever used before overwriting.

This cryptographic service is isolated from the application and vice versa. The random from the cloud has no visibility into how it is used and what is encrypted in which application. Similarly, the application provider has no ability to decrypt the data without

direct access to the same random. The two specialized functions are decoupled, enhancing security for all. With ever-increasing global privacy requirements, this solution separates the service provider from the security guarantors in this example. The same technique can be used to deliver medical records, financial statements and other data from a provider in a compliance industry.

Securing Data at Rest

Securing data with OTP encryption requires fewer computational resources, less power, and is far more secure than other alternatives like AES. The trade-off is the need to store keys that are equivalent in size to the files being encrypted. This makes OTP an ideal candidate for situations where security is paramount, or when low power or minimal compute complexity are valued – such as in battery operated devices.

When designing a data at rest solution, the entropy required to generate your keys must be considered. Trade-offs need to be considered such as network bandwidth and latency requirements for the solution being designed. Unlike computationally secure encryption keys, an OTP must be at least as long as the data to be encrypted. To create this OTP, about twice as much random must be sampled from a source of quantum random numbers to create a local random repository. Often, a much larger set of random and is downloaded and may be used for many encryption keys. For example, if hundreds of 1MB files are typically encrypted a single 1GB random pool would be sufficient — hundreds of individual 1MB pools are not required. Each file to be encrypted applies unique extractors to the same pool to generate inimitable OTPs equal in size but never using the same quantum random twice. Depending on a tunable parameter, no more than 90% of the random pool is ever used, before more random needs to be replenished or a new pool established.

Data encrypted with this technique may be publicly posted or openly transmitted with no security risk – when something is information theoretically secure it isn't possible to be more secure. In order to decrypt the data, the recipient or users must have a means of generating the OTP. This can be by using the Qrypt BLAST protocol included in the Key Generation solution, or by providing the same random pool out of band. This is the standard configuration for an air-gapped system of geographically isolated members. A sufficiently large random pool, perhaps enough for a year, is replicated on SSDs and

mailed or otherwise delivered to every team member. Encrypted files may be sent over email, messaging app, etc, and moved to a laptop disconnected from the internet for decryption. The operating assumption is the files are harvested in-flight, but their capture is irrelevant because they cannot be decrypted.

Securing Data in Transit

The same concepts and techniques used to securely store data at rest can be extended to modern applications like messaging, however end-to-end encryption requires additional mechanisms like “ratchets”, which provide further guarantees like forward secrecy and other highly desirable features. In 2019, Qrypt cryptographer Yevgeniy Dodis published a paper on the details combining these distinct technologies into an integrated PQC solution, demonstrating a quantum-secure protocol for data in transit.

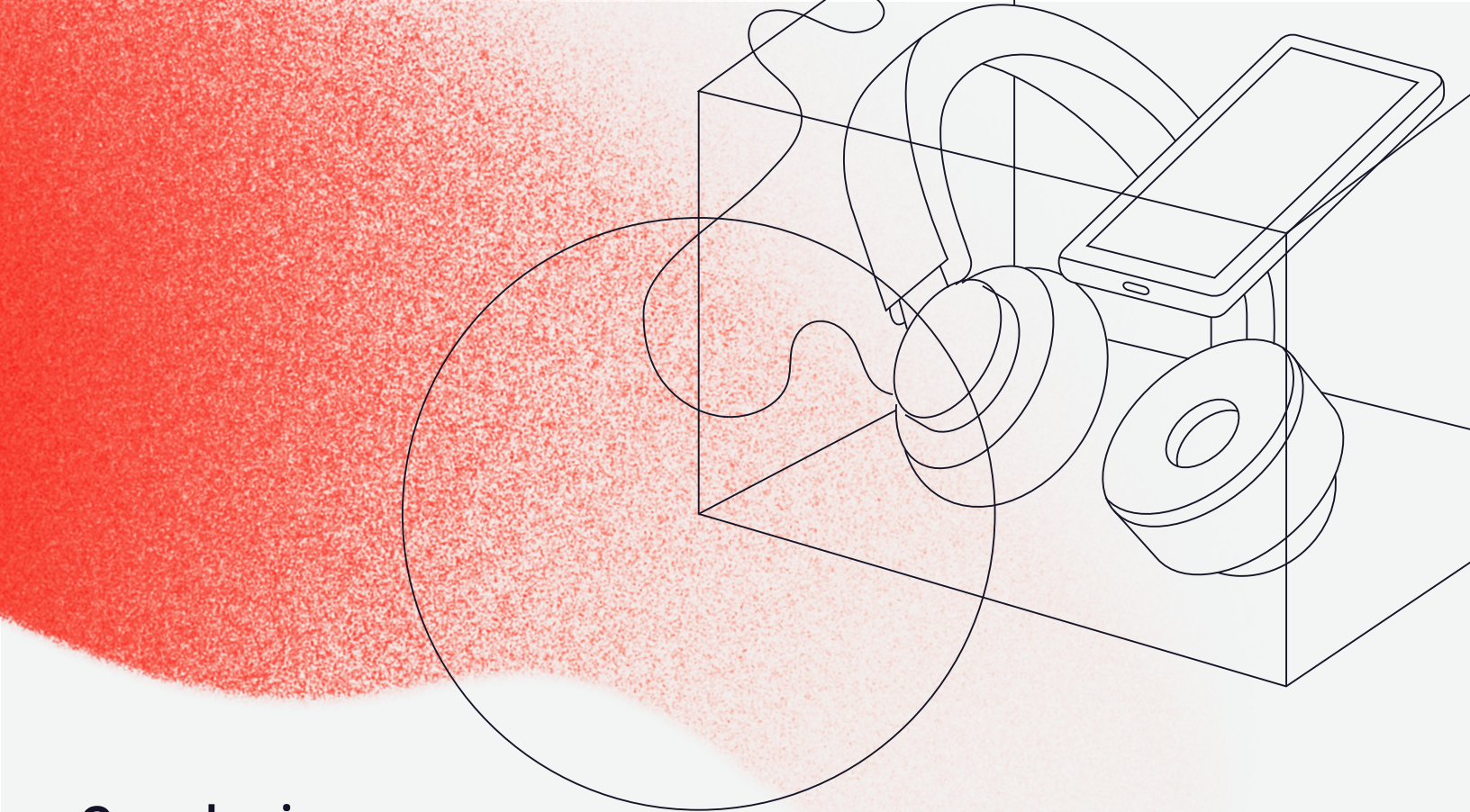
Basic PQC uses an asymmetric algorithm from the NIST competition and the various forms of AES for the symmetric side. The former is only used to make sure two users can agree on the same AES key used to encrypt any amount of data back and forth for as long as required. This describes a simple quantum-resistant solution, however, is not immune to attacks on random, the harvest now and decrypt later attack, or attacks where a hacker is able to compromise an AES key.

Adding a second feature called ratcheting, increases the security level by never reusing the same AES key and continuously cycling through newly made keys for each data transmission. This prevents a hacker who learns one or several of the keys from decrypting all the messages between two users, a property known as forward secrecy.

To further increase security, replacing the asymmetric key distribution with BLAST protects against the harvest now and decrypt later attack. Replacing the AES with OTP increases the level further to quantum-secure, meaning, an unbounded adversary can never break the communique. Each encrypted message or ciphertext may be transmitted in the open without concern for harvesting because there is no brute force attack possible to break it, unlike the AES case. An additional benefit is that encryption is end-to-end (E2E), meaning, no middleman intercept is possible. Encryption and

decryption operations are only possible at the endpoint device, not at intermediary transit locations like ISPs, satellites, and data centers.

The only means of compromising a system designed in this way is if the adversary has full control of a user's device or can monitor and collect all data to it. They would effectively see what the device user sees, and then the security would be computational, not everlasting. However, several of the quantum random sites can be compromised, without an impact to the security of the overall system, given the properties of how OTP encryption works. This cryptographic utility eliminates the single point of failure of most other systems and assumes some of the distributed infrastructure is either monitored or wholly owned by nefarious actors. However, without full control, it is all or nothing. The double ratchet mechanism and continuous generation of ephemeral random guarantees even temporary access to some OTPs/keys only allows attackers limited access to some data, with full security restored quickly.



Conclusion

The future of cyber security is uncertain due to the ever-increasing rate at which technology is progressing – and hackers with access to these technologies have an asymmetric advantage over those trying to secure our secrets. Qrypt provides solutions for entropy, key generation, and secure transfer that help even the odds. They can be integrated into applications or infrastructure to make them quantum-secure, by leveraging cloud infrastructure, innovative protocols, and high-rate Quantum Random Number Generators (QRNGs). And for the first time, One Time Pad encryption is practical, available to anybody, and accessible globally.



Contact Qrypt today.

To learn more about how Qrypt can help you prepare for the quantum age, visit www.qrypt.com or email info@qrypt.com