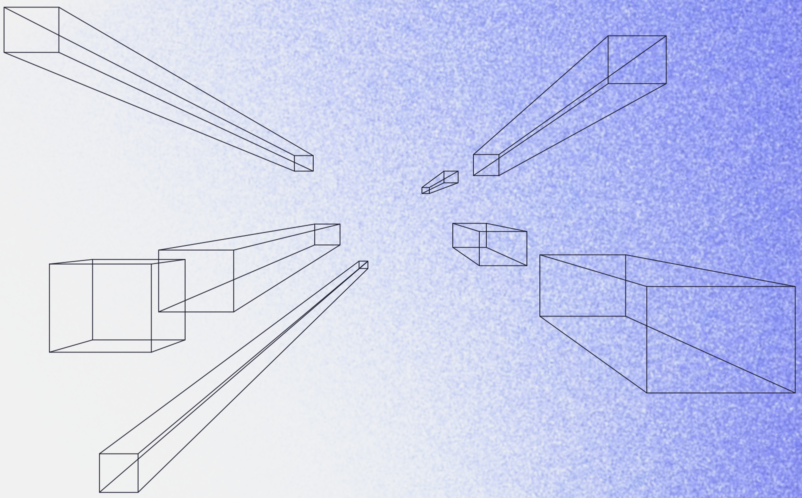
Qrypt

Quantum Entropy

Quantum-generated random numbers to improve key security and eliminate entropy starvation.



The Illusion of Randomness

Randomness is the cornerstone of digital security. It's the unpredictable variable that fortifies our security systems, making them impenetrable to attacks. But what if the randomness we rely on is merely an illusion?

Traditional random number generators (RNGs), whether they are hardware-, firmware-, or software-based, are not truly random. They are deterministic, following a set pattern or algorithm. While these patterns may seem random at first glance, they can be predicted with enough computational power and knowledge of the algorithm. This predictability limits the key space, the range of potential random numbers that can be generated. If an attacker can figure out the algorithm and the seed value, they can predict all future numbers that the RNG will produce, leading to a potential security breach.

In contrast, quantum random number generators (QRNGs) leverage the inherent randomness of quantum mechanics to generate truly random numbers. The numbers produced by a QRNG are unpredictable and cannot be replicated, providing an essentially unlimited key space. This makes QRNGs ideal for tasks that require high security, such as encryption.

Classical and pseudo RNGs pose an immediate vulnerability in our security infrastructure, enabling skilled attackers to exploit predictability and cause potential breaches and data compromises.

Limited Key Space of Classical RNGs

Classical RNGs, both hardware and firmware-based, derive randomness from classical physics, not quantum mechanics, limiting the key space and making them potentially predictable if algorithms and seed values are discovered.

Unlimited Key Space of QRNGs

Quantum RNGs, on the other hand, leverage the inherent randomness of quantum mechanics. This allows them to generate truly random numbers with an essentially unlimited key space. The numbers produced by a QRNG are unpredictable and cannot be replicated, making them ideal for tasks that require high security, such as encryption.

Security Implications

Classical and pseudo RNGs pose a tangible security risk due to their limited key space and vulnerability to prediction, potentially enabling encryption breaches. While they lack robust forward and backward security, QRNGs, with their unlimited key space and inherent unpredictability from quantum mechanics, assure a superior security level, safeguarding both past and future states even if a single state is compromised.

The Present and Pervasive Risk to Cryptography

The illusion of randomness in classical RNGs is not merely a theoretical concern but a present and pervasive risk, with tangible implications leading to significant security breaches. As Auguste Kerckhoffs, a 19th-century cryptographer, emphasized, "***A cryptosystem should be secure, even if everything about the system, except the key, is public knowledge***." However, if the key — derived from ostensibly 'random' numbers — is compromised, the entire system is jeopardized.

Historical instances of RNG failures underscore this risk, revealing vulnerabilities that have led to substantial breaches in cryptographic systems. These failures, ranging from backdoors inserted by national agencies to bugs in widely-used cryptographic libraries, have exposed the limitations and potential dangers of relying on classical RNGs. Such instances have not only compromised user data but also undermined trust in digital security protocols and systems.

The subsequent sections will explore a quantum solution that provides true randomness, thereby securing our cryptographic systems against both current and future threats.

Auguste Kerckhoffs
Cryptographer, 19th Century

ENTROPY AS A SERVICE

Why Use an EaaS

The vast majority of cryptographic solutions, if not all, do not utilize true quantum entropy today. You can immediately improve your security posture by leveraging EaaS to provide an unlimited entropy source to your key generation, management, and other security solutions.

Additionally, if you are including an EaaS service already, NIST strongly recommends that "at a minimum two independent EaaS instances located in different geopolitical locales be used as remote sources." Qrypt can be the sole source or secondary entropy solution to any security architecture today.

Understanding the pivotal role and immediate applicability of EaaS in enhancing cryptographic security, let's delve into the quantum solution that ensures the provision of true, unassailable randomness in the generation of cryptographic keys and other security applications.

The Quantum Solution

The limitations of classical and pseudo RNGs and the risks they pose to our security infrastructure necessitate a more robust solution. Enter quantum random number generators (QRNGs). QRNGs leverage the inherent unpredictability of quantum mechanics to generate truly random numbers. Unlike their classical counterparts, QRNGs are not deterministic; they do not follow a set pattern or algorithm that can be predicted. This makes them ideal for tasks requiring high-security levels, such as encryption.

True Randomness

Quantum mechanics is the only known source of true randomness. Classical RNGs only simulate randomness and are susceptible to side-channel attacks as may be predicted by a classical computer. In contrast, QRNGs, due to the inherent unpredictability of quantum phenomena, are both less susceptible to side-channel attacks and generate numbers that are truly random and unpredictable.

Unpredictability

The numbers produced by a QRNG cannot be predicted or replicated. This unpredictability is a result of the inherent randomness of quantum mechanics, not a product of a complex algorithm or large key space.

High-Quality Entropy

The quality of entropy is crucial for the security of cryptographic systems. QRNGs provide high-quality entropy, ensuring that their random numbers are truly random. This high-quality entropy is essential for the generation of secure cryptographic keys.

Verification

The methodology for generating quantum random numbers should be publicly disclosed and subject to critical review by engineering professionals. It's essential to validate and verify that the output random distribution aligns with the quantum mechanical theoretical model specific to the chosen quantum process. This ensures that the RNG is not only truly random but also adheres to the expected physics of the implemented approach, reducing the risk of deterministic behavior that attackers could exploit. This is a crucial point.

Testing

Rigorous testing should be conducted to analyze the entropy source and the electronics used to digitize the output. This testing should establish the ratio of quantum signal to classical noise in the device and confirm the expected results.

Randomness Extraction

After the raw output of random numbers has been validated, randomness extraction is employed to remove any classical contamination that might degrade the quantum entropy. This step ensures a heightened degree of randomness and unpredictability in the final output.

With QRNGs, we can move beyond the illusion of randomness and towards a future where our security systems are fortified by true randomness. In the next section, we will explore how Qrypt is leading the way in this quantum revolution.

Strong Partnerships with Prestigious Labs

Qrypt's unwavering commitment to quantum security is exemplified through our strategic partnerships with renowned national and international research institutions. Both technologies are patented by their respective national labs and are exclusively licensed to Qrypt.

Qrypt's QRNGs are not only at the forefront of quantum security but are also assembled in the US, ensuring a controlled and secure supply chain, vital for US-based companies. This collaboration aligns perfectly with the US Government's heightened focus on addressing quantum threats to national security, as evidenced by recent directives and executive orders.

OAK RIDGE National Laboratory

Our collaboration with ORNL has been particularly fruitful, leading to the development of a Quantum Random Number Generator (QRNG). This QRNG, designed and assembled entirely in the US, utilizes quantum fluctuations of optical signals to produce genuine randomness. The expertise ORNL brings in quantum information science significantly enhances the reliability and robustness of Qrypt's QRNG.

Los Alamos NATIONAL LABORATORY

Our partnership with LANL has yielded significant advancements in QRNG technology, rooted in the intricate quantum physics of matter and light at the atomic scale. Qrypt's selection for this project, after a rigorous competitive process, underscores our deep expertise in cryptography and our ability to address pressing market needs. The technology developed in collaboration with LANL, backed by a Cooperative Research and Development Agreement (CRADA), has undergone meticulous peer review, ensuring a robust scientific foundation for our quantum initiatives. This partnership not only highlights our commitment to cutting-edge R&D but also aligns with the US Government's focus on quantum security, as evidenced by recent directives and executive orders.

EPFL ICFO

In addition to ORNL and LANL, Qrypt maintains strong ties with other prestigious institutions, including École Polytechnique Fédérale de Lausanne (EPFL) and The Institute of Photonic Sciences (ICFO). Our exclusive technology licenses, robust global patent protection, and a portfolio of peer-reviewed publications further emphasize our dedication to advancing the frontiers of quantum security.

The Qrypt Advantage

Qrypt stands at the forefront of quantum security, offering distinct advantages with our Qrypt Quantum Entropy, a leading Entropy-as-a-Service (EaaS), and our Quantum Random Number Generators (QRNGs).

Multiple Quantum Sources

At Qrypt, we understand the importance of robustness and reliability in generating quantum randomness. Our Quantum Entropy (EaaS) utilizes multiple independent sources of quantum randomness. This approach ensures the production of high-quality random numbers and eliminates the possibility of a single quantum source or its supporting electronics being characterized or predictable. The combined random numbers from these sources are XORed to create a super entropy, enhancing the security and reliability of our EaaS for high-security applications.

Seamless Integration with Existing Infrastructure

Qrypt's solutions are designed to enhance your security posture without the need to overhaul your existing systems. Leverage your current infrastructure and integrate our EaaS seamlessly, ensuring an immediate improvement in your security capabilities without significant investments in new hardware or software.

Quick and Easy Implementation

Experience the ease and speed of adopting Qrypt's EaaS. With straightforward integration options and a globally available service, your organization can be up and running with enhanced quantum security in no time. Whether utilizing APIs, PKCS#11, rng-tools rngd, or HashiCorp Vault Entropy augmentation, Qrypt ensures a smooth and swift implementation process. Additional integrations are planned, and customers can request solutions for their bespoke implementations.

Cost-Effective Quantum Security

Enhance your security without hefty investments in new hardware or software. Qrypt's EaaS is not only efficient but also cost-effective, providing your organization with a robust, reliable source of true randomness without straining your budget.

Generate Massive Quantities of Secure Keys

With 1 GB of quantum entropy, you can generate a staggering 31,250,000 AES-256 keys, ensuring a vast, secure key space for your cryptographic needs. This immense capability fortifies your security and provides a virtually inexhaustible source of true randomness for generating secure cryptographic keys.

Fast, Globally Available, and Scalable

Qrypt's EaaS is designed to provide random numbers quickly and efficiently. Our globally available service ensures users from various locations can access high-quality quantum randomness seamlessly. Moreover, our infrastructure is built to handle extensive random number generation requests, catering to both small-scale and large-scale applications.

Domestic QRNG Assembly for Enhanced Security

Qrypt QRNGs are developed and assembled entirely in the US. This domestic assembly ensures a secure, tamper-proof supply chain, which is vital for security. Our collaboration with the national labs also highlights our dedication to cutting-edge U.S. R&D, emphasizing the importance of domestic technology development in alignment with national security interests.

Qrypt's Quantum Entropy EaaS offers multiple quantum sources, fast and globally available service, scalability, and flexible integration options. These advantages make Qrypt's EaaS a reliable and secure choice for applications requiring high-quality random numbers. As we continue to innovate and push the boundaries of quantum security, we remain committed to providing our users with the most secure, robust post-quantum cryptography solutions.

Getting Started with Qrypt

Unlock unparalleled cryptographic security with Qrypt's Entropy as a Service (EaaS), delivering high-quality quantum entropy directly to your applications, wherever they reside. Qrypt's EaaS is not merely a source of true randomness but a pivotal enhancer of robust, unassailable security across your cryptographic systems and applications.

Achieve Unparalleled Security Outcomes with Qrypt:

- **Fortify Cryptographic Systems:** Enhance the security of your cryptographic keys and systems by integrating true quantum randomness.
- **Bolster Data Protection:** Safeguard your data by ensuring that encryption keys are generated with the highest quality of entropy, making them impervious to predictive attacks.
- **Secure Communications:** Ensure secure, private communications across your networks by utilizing quantum entropy in key generation and management.

.

1 Identify Integration Points

Determine where quantum entropy can enhance your existing security systems, such as in key generation and management.

2 Choose Your Integration Method

Utilize Qrypt's flexible integration options, including APIs, rng-tools rngd, and HashiCorp Vault, or leverage ask our experts for help.

By embracing EaaS, you can leverage true quantum entropy to immediately bolster your security. **Whether you're looking to enhance your existing security solutions or build new ones,** Qrypt's EaaS provides a robust, reliable source of true randomness that can meet your most demanding needs.

SECURE YOUR IT INFRASTUCTURE TODAY

CONTACT QRYPT

www.qrypt.com