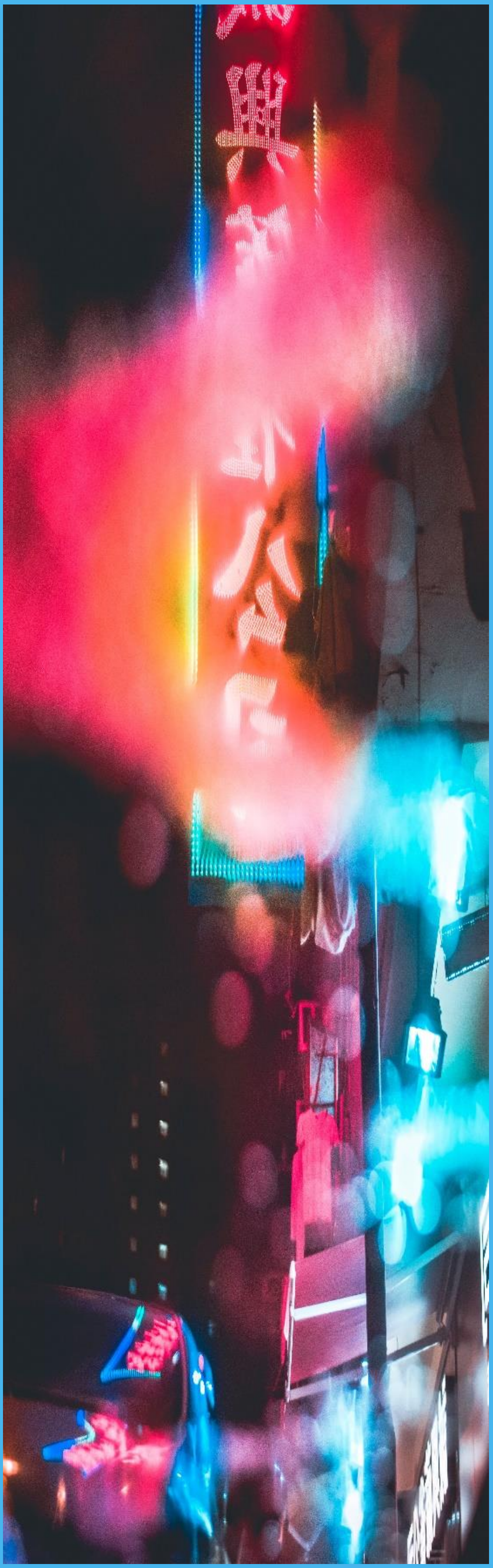


Quantum Cyber Security:

Security solutions for the future, delivered today.

Suretech Company Limited

March, 2022

Suretech Company Limited, at a glance:

Suretech Company is Asia’s first cryptographic key generation platform based on verifiable quantum randomness. It is designed to secure the world’s data from both current and advancing threats to today’s encryption.

Suretech’s solution is a cloud-hosted platform that uses the unpredictable nature of quantum mechanics to generate superior cryptographic keys. Each key is seeded with verifiable quantum randomness drawn from quantum computers. The platform supports traditional cryptographic algorithms, such as RSA or AES, as well aspost-quantum algorithms currently being standardised by the National Institute of Standards and Technology (NIST).

https://www.quantum-cybersec.com https://www.suretechcompanylimited.com

THREATS TO MODERN ENCRYPTION

Cyber security relies on multiple layers of defense to defeat attackers. The foundation of these layers is the cryptographic keys that encrypt sensitive information.

Strong cryptographic keys must be completely unguessable to an attacker. This means the creation of high-quality randomness is at the heart of key generation. Today, companies use cryptographic keys that are not truly random. In one recent study, researchers uncovered nearly half a million certificates in active use that are so fundamentally weak, they can easily be broken by today's computers.

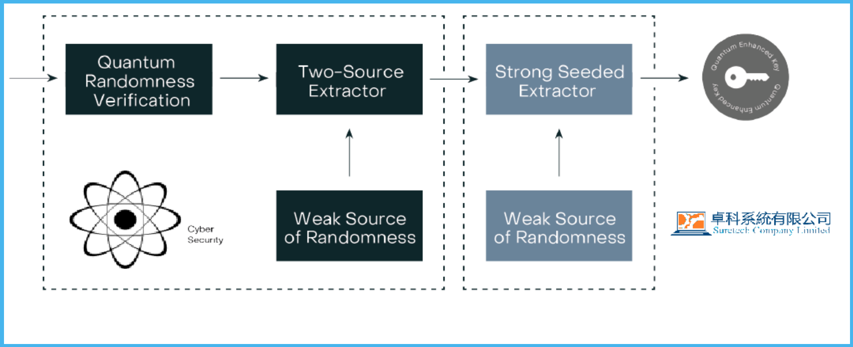
The problem is caused by existing RNGs, which cannot generate verifiable randomness.

HACK NOW, DECRYPT LATER

In the future, quantum computers will be able to break many of the encryption systems we rely upon today. Because a powerful quantum computer doesn't exist yet, many companies mistakenly believe the data they exchange today is completely safe, provided it's encrypted.

A "hack now, decrypt later" attack involves intercepting and recording encrypted data as it passes through public networks. When a powerful quantum computer arrives, which may only be 5-10 years away, according to Google's CEO, the attacker can retrospectively break the encryption used to protect the data.

To defend against this attack, companies can move towards using quantum-safe encryption algorithms, such as those being standardized by the NIST post-quantum cryptography process.



Suretech's solution has been designed to support those algorithms from launch, helping customers to transition towards solutions that are resistant to quantum attack.

SURETECH COMPANY LIMITED, A UNIQUE APPROACH

Every key generated by Suretech is seeded4 from verifiable quantum randomness. The word “verifiable” is crucial because it’s the reason Suretech delivers superior security guarantees compared with other solutions in the market.

Suretech’s random number generation leverages nature’s intrinsic randomness. According to the laws of quantum mechanics, qubits can be prepared and measured in such a way as to produce an outcome of “0” or “1” with exactly 50% probability. Unlike other solutions on the market, Suretech is able to isolate this randomness from deterministic classical noise without relying on strict modelling of the device. The result is mathematically-proven, near-perfect randomness, which is used to generate superior cryptographic keys.

Other solutions may claim to generate exceptional randomness; however, those claims are rooted in unfair assumptions about how those devices are constructed and how they operate.

Because the Suretech approach is based on a device independent protocol, we can verify our randomness is as good as we claim it is.

The Suretech platform uses a quantum computer to generate quantum-enhanced randomness.

Using entangled qubits and the Bell Test, we verify the level of randomness present and further refine the output using multiple randomness extraction operations. This ensures a near-perfect set of randomness is available for cryptographic key generation.

EASY INTEGRATION, SECURING SYSTEMS TODAY AND TOMORROW

As Suretech’s solution is a cloud-hosted platform, it integrates easily with existing cryptographic systems such as virtual private networks, hardware security modules, public key infrastructure, or any cryptographic system where keys are consumed.

Suretech’s customers request new cryptographic keys by calling a web API. The response is an encrypted key, which can be securely imported into existing cyber security systems.

Suretech then generates standard cryptographic keys, such as those used in AES or RSA, as well as those used in post-quantum algorithms. This means the platform can help increase the security of today’s systems, while being future-proofed for the pending transition to post-quantum algorithms.

By using our solution, companies can help reduce the risk of data breaches caused by weak or inferior keys across a wide range of use cases, see on the right side.

- Hybrid Encryption
- Data Watermarking
- Data at Rest
- Identity & Access Management
- Blockchain
- Data in Transit
- Secure Messaging
- Internet of Things
- Raw Randomness

THE RESEARCH BEHIND SURETECH COMPANY LIMITED

The Suretech team is supported by a research group with a long history of academic success.

The researchers led by Prof. Jianwei PAN (潘建伟), from the University of Science and Technology of China, have successfully built a quantum computer that is able to perform certain computations nearly 100 trillion times faster than the world's most advanced supercomputer, representing the first milestone in the country's efforts to develop the technology.

With collaborations from the Synergetic Innovation Center of Quantum Information, National High Performance Computing Center and CAS Key Laboratory of Quantum Information all located at University of Science and Technology of China.

PATENTS

The technology underpinning Suretech Company Limited's solutions are patented. Further implementation-specific patents are pending.

Want to know more? Contact us, and one of our experts will get back to you:
info@quantum-cybersec.com
inquiry@suretechcompanylimited.com