www.eylpartners.com

QUANTUM ENTROPY GAME CHANGER FOR IoT SECURITY

EVERYWHERE IN YOUR LIFE

Quantum Entropy : The Ultimate Randomness Nature Has to Offer.

EYL's QUANTUM™ devices exploit an intrinsic process in nature to heighten ICT and IoT application security.

EYL applies the natural process of radioisotope decay, commonly used in consumer medical devices, smoke detectors, and watches, to the use case of cryptographic information security. By exploiting the true randomness (entropy) of this quantum process, EYL's technology brings optimal security protection to a wide range of ICT and IoT products, at an affordable price. It's a game changer.

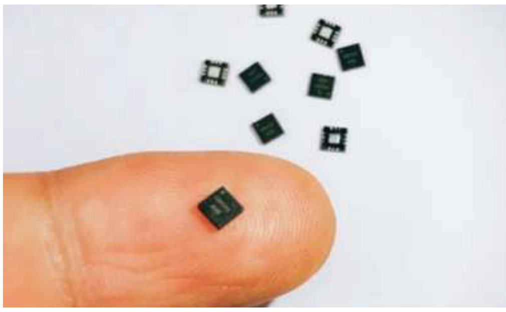
Random number keys are a primary component of cryptosystems used to keep internet communications and digital data safe from hackers. The resistance of these systems against hackers is governed, in part, by the entropy strength of their random number generators. Today, most encryption systems use software-generated cryptographic keys for convenience and speed, but at the expense of yielding lower entropy, consequently increasing their vulnerability to attack.

EYL offers a hardware-based, quantum entropy source and quantum random number generator technology that is the smallest, cheapest, fastest, and lowest power solution in the market. Because the source of randomness comes from quantum phenomenon, it is always truly random, by the laws of quantum physics, enabling the highest level of cryptographic security.

The QUANTUM™ Random Number Generator (QRNG) product family from EYL is designed to directly address the convergence security demands introduced by the 4th Industrial Revolution and the new generation of connected IoT devices and systems.

EYL has developed

"The world's smallest, cheapest, fastest and lowest-power QRNG!"



"The QUANTUM™ Random Number Generators from EYL - securing the future!"

QUANTUM™
Random Number Generator

Quantum

At its core is the QUANTUM™ Entropy Chip, the first quantum security solution at your fingertips.

2

Today's IoT security solutions must take on the same design requirements imposed upon the connected devices they protect. They should be small, reliable, inexpensive, consume little power, yet address ever evolving and stronger external threats. EYL's QUANTUM™ products meet these demands. They perform key crypto functions and are packaged in various form-factors to address a wide range of market applications.

Other commercial hardware quantum RNG solutions use optical processes to provide a high-speed quantum entropy source. These tend to be expensive and bulky, narrowing their use to server-based authentication and encryption platforms, rather than the growing number of edge devices in IoT applications.

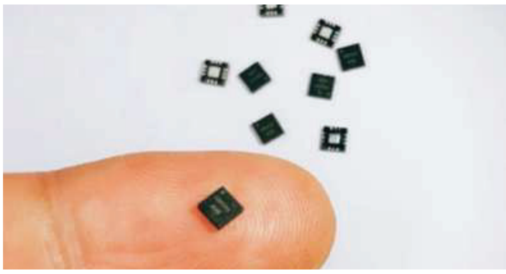
EYL's family of QUANTUM™ products includes the QUANTUM Entropy Chip (QEC) and QUANTUM™ Random Number Generator (QRNG) in flip-chip, USB and PCI card formats, supporting RNG speeds of up to 4 Gbps! The roadmap also includes a QUANTUM™ Cryptography Chip (QCC) that performs real time encryption of digital input data streams. The QCC is the world's first chip to integrate cryptographic algorithms and Side Channel Attack defenses with QRNG technology.

EYL's QUANTUMTM Entropy Chip SCA resistant version(QECS), extends the capabilities of its groundbreaking, miniaturized QEC device, to include Side Channel Attack resistance. Boasting a tiny, low-profile, 3mm square SoC form factor and hardened physical attack protection, the new device defends against power analysis threats and etc., while maintaining the low-power and high-performance characteristics that made its predecessor so compelling a device. Used as an ideal, Quantum Random seed source for random number generators, QECS delivers the ultimate randomness that empowers cryptosystems to reach their highest security potential. Just what EYL's QUANTUM™ technology is known for.

EYL's QUANTUM™ Devices

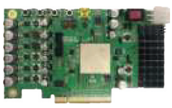
QUANTUM Entropy Chip

+ QEC SoC
+ QECS(SCA resistant function)



QUANTUM Random Number Generator

+ QRNG (SoC, USB, PCI)



QUANTUM Crypto Chip

(concentual)

"QCC is the first Crypto-chip integrating Side Channel Attack defense with QRNG technology."

End-to-end security mechanisms in the on-line, digital services environment must be initiated at login and operate continuously. As a compliment to its device portfolio, EYL offers system-level, QUANTUM™ security solutions, to realize these requirements.

MOTP™: Mobile Cloud OTP Authentication System

A QRNG-secured, One Time Password system with mobile phone authentication.

Through MOTP, mobile phone OTP authentication is added to the PC user's ID/PW login, for added security. The authentication server sends a QRN-generated "challenge" number to the user's mobile phone and confirms system login only after the user returns the identical challenge back to the server.

QLock™: Simple and Secure Pattern Lock Protection

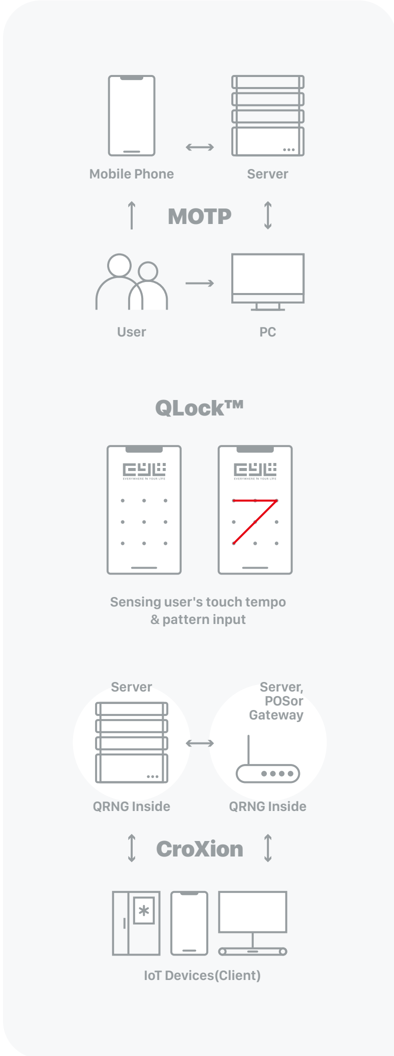
EYL's patented solution, developed to defend Pattern Lock authentication schemes, popular with Android users, against various security threats.

Dynamic password methods and user behavior detection algorithms are used to protect against snooping and replay attack exploits. QLock™ defenses can be extended to also avert Smudge, Thermal and Man-in-the Middle Attacks in support of FinTech and IoT-based services.

CroXion™: The Multi-point Cross-Certification System

A multi-channel authentication system via QRNG security.

With QRNGs installed in devices and servers, cross-certification is performed to establish a Trusted Network, using a bit stream of random numbers generated by all devices after login to establish a Trusted Network. Continuous, real-time authentication is conducted at least once every second to ensure the communication integrity.



Quantum

Stronger Entropy, Highest Standards

Our quest for true randomness and unbreakable encryption

4

FULLY TESTED AND FOUND COMPLIANT

Our quest for true randomness and unbreakable encryption led to the development of the QUANTUM™ product portfolio. In developing this pioneering technology, we also needed to create real-time entropy testing software, and of course, our QEC and QRNG products passed with flying colors! But don't take our word for it. Our products have been independently tested and are compliant with the randomness testing standards below.

+ NIST SP 800-22 : Statistical Test Suites for Deterministic Random Number Generators for Cryptographic Applications
+ NIST SP 800-90B Recommendation for the Entropy Sources Used for Random Bit Generation, Validated from FIPS 140-2
+ AIS.31 : A proposal for Functionality Classes and Evaluation Methodology for True (Physical) Random Number Generators. Version 3.1
+ DIEHARD Tests

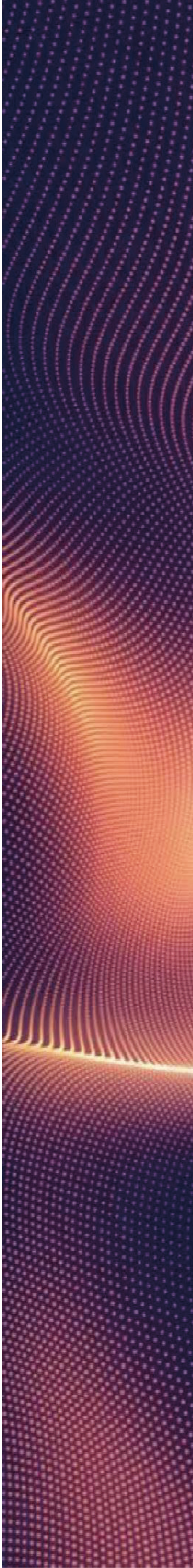
BACKED BY STRONG PATENT PORTFOLIO

EYL boasts a rich patent portfolio for the QUANTUM™ family of products and processes.

Patent Portfolio

+ 6 global PCTs pending
+ 10 Korean patents issued
+ 8 Korean patents pending
+ 3 US patents issued
+ 2 US trademark and 5 Korean trademarks issued
+ 2 Korean trademarks pending

EVERYWHERE IN YOUR LIFE



KOREA OFFICE

Junghyun "Francis" Baik
CMO

Office : +82.2.6933.7190
Mobile : +82.10.3168.1418(Korea) E
-Mail :contact@eylpartners.com

4F 7-40, Mabang-ro 6-gil, Seocho-gu
Seoul, 06776, Republic of Korea

www.facebook.com/eylkor

www.linkedin.com/company/eylpartners