QEC – The QUANTUM™ Entropy Chip

EYL's pioneering QUANTUM™ technology harvests ultimate randomness (entropy) from nature using radioisotope decay. Core to this technology is the QUANTUM™ Entropy Chip, or QEC – the first quantum security solution at your fingertips. Boasting a tiny, low-profile, 3mm square SoC package and low power consumption, it is the ideal, truly random seed source for random number generators used in advanced cryptographic systems.

QEC delivers the ultimate randomness to empower these cryptosystems to reach their highest security potential. And it delivers this in a package that meets the new performance demands imposed by emerging ICT and IoT applications.

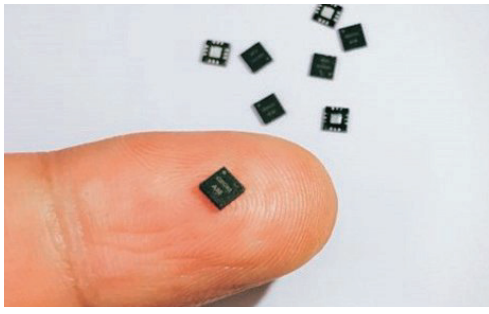
QEC is EYL's commercial quantum entropy chip, available in a flip-chip form factor. QECS, EYL's 3rd generation entropy chip, extends the performance and hardened physical attack protection of its predecessor device, to include Side Channel Attack protection.

EYL incorporates its high entropy QEC into its QUANTUM™ Random Number Generator family of products. This produces the lowest cost, most versatile, Quantum random number generator (QRNG) solutions in the market, able to support the widest range of 4th industrial revolution use cases.

General Specifications

Operating Temperature	-20°C to +85°C
Voltage	3.3 Volts
Current	800 uA
Form Factor	SoC flip-chip
Dimensions	2mm(L) * 2mm(W) * 0.8mm(H)

Quantum Entropy Chip



Key Features

+ Quantum randomness
+ Ideal RNG seed
+ Miniature form factor SoC
+ Low power, Low cost
+ NIST SP800-90B compliant
+ SCA protection

ASIA & EUROPE
Tel : +82.2.6933.7190
E-Mail : contact@eylpartners.com

US & CANADA
Tel : +1.703.682.7018
E-Mail : contact@eylpartners.com

QUANTUM™ Random Number Generator

Quantum

Ultimate randomness at your fingertips

EVERYWHERE IN YOUR LIFE

EYL has developed a new generation of true random number generators. They are built upon their unique and innovative technology that exploits the true randomness (entropy) in the quantum process of radioisotope decay.

Random number generators (RNGs) are essential components of many cryptosystem applications, including encryption, authentication, and digital signing, all used to keep internet communication and digital data safe from hackers. Their level of security protection is directly related to the entropy strength of the RNG.

The high randomness yielded by EYL's QUANTUM™ technology raises the bar on security protection, at a very affordable price.

EYL offers a versatile product portfolio of QRNGs that support various form factors, operating speeds and interfaces to address the ever-growing number of crypto applications in the digital world.

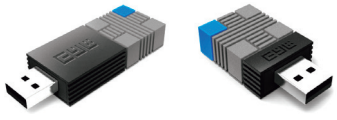
General Specifications (USB)

Parameter	QRNG-H	QRNG-L
Speed	1.0 Gbps	1.0 Kbps ~ 1.0 Mbps
Operating Temperature	-20°C to +85°C	-20°C to +85°C
Voltage	5 Volts	5 Volts
Current	125 mAmps	60 mAmps
USB Dimensions	65 mm. * 23 mm. * 10 mm.	44 mm. * 11 mm. * 23 mm.

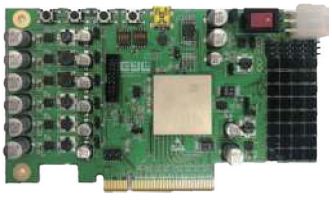
General Specifications (PCI-express)

Speed	4 Gbps
Operating Temperature	0°C to +60C
Voltage	5 Volts
Dimensions	120 mm. * 100 mm.

High Speed, Low Speed USBs



PCI -e card



Key Features

+ Quantum randomness
+ Low power, Low cost
+ High speed
+ SCA protection
+ NIST SP800-22 compliant
+ AIS.31 compliant
+ DIEHARD tested

Applications

+ Ciphering
+ Authentication
+ Digital signatures
+ IoT device security
+ Gaming
+ Blockchain
+ Secure printing

ASIA & EUROPE
Tel : +82.2.6933.7190
E-Mail : contact@eylpartners.com

US & CANADA
Tel : +1.703.682.7018
E-Mail : contact@eylpartners.com

QCC - Quantum Crypto Chip

Quantum

Our mission is to strengthen cyber security of connected devices and data by providing a more secure and affordable platform

EVERYWHERE IN YOUR LIFE

EYL 's quantum random number generator can be applied to cryptography directly and we are continuously innovating to find the best application for its use, including a unique patented authentication system. EYL's high quality random numbers also provide a platform that can be applied to broad range of solutions for diverse purposes. We are developing solutions at the speed of light because we collaborate with our partners.

The following is an Quantum Crypto Chip of EYL's products and solutions being applied meaningfully. EYL is developing the world's first strong cryptographic chip (QCC) with quantum random number generation technology, side channel attack protection technology and malware defense technology. Prototype launch in 2019, mass production in 2020.

Once the implementation of the function is completed, it will be released as a 5mm x 5mm chip through the SoC process. QCC is developed for use in all devices requiring security, and is developed as a powerful security chip with fast information throughput and low power.

General Specifications (QCC)

Processor	32-bit Cortex-M4
Operating Temperature	-20℃ / +80℃
Power	3.0V to 3.6V
Operating frequency	Up to 100MHz
Secure I/O Management	IOMMU : Input/Output Management Unit
Package	144-Pin LQFP

The areas of potential application of the QCC are Dron, FIDO2 Authentication, AP (Access Point), Print cartridge, GPS, Navigation, Mobile Device, IPTV, CCTV, Set-Top Boxes (STBs), Etc.

QCC

(concentual)

Key Features

+ Quantum randomness
+ Ideal RNG seed
+ Miniature form factor SoC
+ Low power, Low cost
+ CTR-DRBG SP 800-22 compliant
+ NIST SP800-90B compliant
+ Asymmetric, Symmetric cipher function
+ Hash AlgorithmSide Channel Attack Resistance

ASIA & EUROPE
Tel : +82.2.6933.7190
E-Mail : contact@eylpartners.com

US & CANADA
Tel : +1.703.682.7018
E-Mail : contact@eylpartners.com

QHSM - Quantum Hardware Security Module

EYL 's quantum hardware security modules (QHSM) applied QRNG technology to implement stronger security functions and developed chip type QHSM to maximize application convenience and efficiency. Like QCC, QHSM is developed for use in all devices requiring security, and is developed as a powerful security chip with fast information throughput and low power.

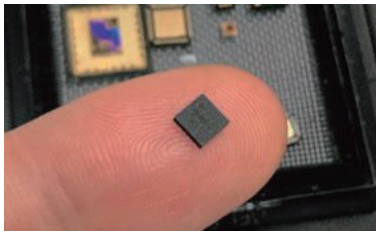
Hardware Security Modules(HSMs) are dedicated devices that are responsible for generating and storing encryption keys. The reason for using HSMs is to achieve all three goals: security, performance, and management. Information contained in the HSM is not inherently copied or reproduced externally.

General Specifications (QHSM)

Processor	32-bit ARM Cortex-M0 Core
Clock	Built in OSC. Main Clock: 50/200 MHz
Reset	Built in power on reset, Software reset
Power	1.5V, 3.3V Supply Voltage
Low Power Consumption Mode	The GPIO is sufficient to power up and down PMU clock gating of Cortex-M0
Package	QFN 4×4-25L (4mm × 4mm × 0.75mm)

The areas of potential application of the QHSM are Print cartridge, GPS, Navigation, Mobile Device, IPC, CCTV, DVD, Set-Top Boxes (STBs), Etc.

QHSM



Key Features

+ Quantum randomness
+ Low power, Low cost
+ High speed
+ Asymmetric, Symmetric cipher function
+ Crypto Device Function
+ Hash Algorithm
+ ECC, RSA FIPS 186-3, 186-4 compliant
+ AES-128/256 FIPS 140-2 compliant
+ SHA-256 FIPS 180 compliant
+ QRNG NIST SP 800-90B compliant

ASIA & EUROPE
Tel : +82.2.6933.7190
E-Mail : contact@eylpartners.com

US & CANADA
Tel : +1.703.682.7018
E-Mail : contact@eylpartners.com

THE service environment provided through IoT is established through connection between devices with various security levels. The security level of all related devices needs to be leveled up at the point of login and during the service. MOTP and CroXion security solutions based on quantum random number generator will do this well.

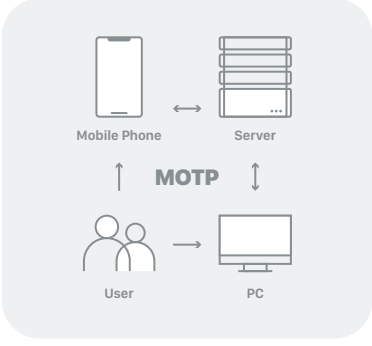
QRNG Secured cloud OTP authentication system

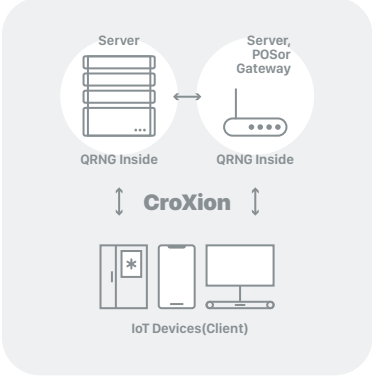
Quantum random number secured One Time Password system : Additional authentication via user's mobile phone

How Does It Work?

If you request OTP after entering ID and PW on your PC, the authentication server checks the user information.

After confirmation, it sends the authentication number based on the quantum random number to the user's mobile phone. The login is completed by accepting the authentication number that the user received from the mobile phone. Through MOTP, mobile phone OTP authentication is added to ID / PW login, which further enhances security.





Multipoint Cross Certification system "CroXion"

Quantum random number secured multi-channel authentication : real-time and continuous

How Does It Work?

A quantum random number generator is installed in a server and a client. Cross-certification is performed using a bit stream of random numbers generated by each device after login to establish a Trusted Network. Real time authentication is conducted at least once every second to ensure the communication integrity.

ASIA & EUROPE
Tel : +82.2.6933.7190
E-Mail : contact@eylpartners.com

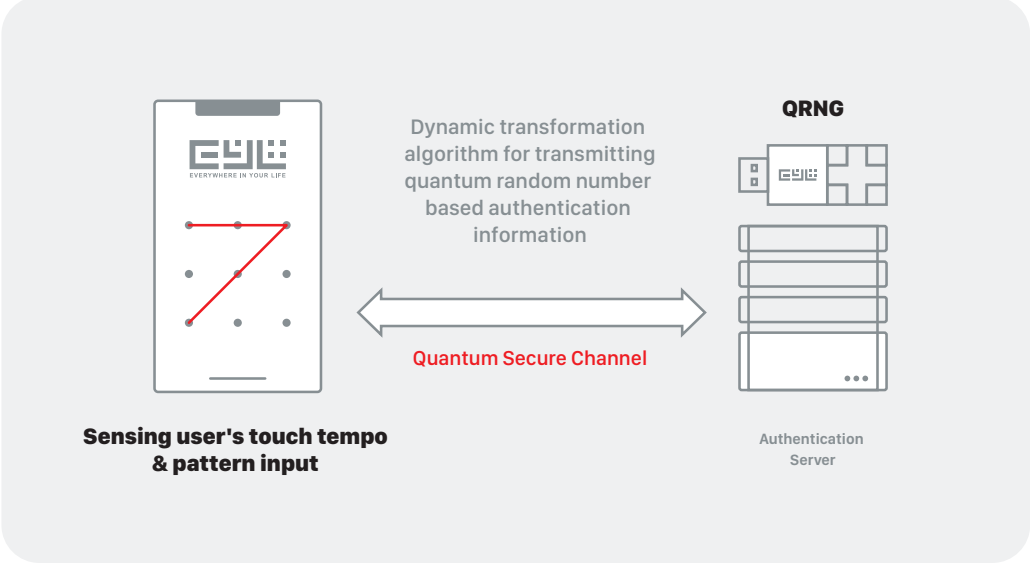
US & CANADA
Tel : +1.703.682.7018
E-Mail : contact@eylpartners.com

Pattern-Lock is one of graphical authentication schemes that shows high popularity today.

+ Pattern Lock is a scheme that utilized 3×3 grid and usually numbered from 1 to 9
+ Touchscreen technology has triggered the implementation of graphical authentications on smartphone
+ Graphical authentication is more fun to use and relative easier to use without needs to create complex alphanumeric combinations

But, user-friendly pattern authentication generally has a weakness in security due to peeping, man-in-the-middle attack, retransmission attack, etc. If this limitation can be overcome, the pattern lock system will satisfy both good user convenience and security.

EYL's QLock is a new pattern authentication method using dynamically generated and transmitted quantum random numbers to defend against Smudge, Shoulder Surfing, Thermal, Man-in-the-Middle, Credential Stuffing.



ASIA & EUROPE
Tel : +82.2.6933.7190
E-Mail : contact@eylpartners.com

US & CANADA
Tel : +1.703.682.7018
E-Mail : contact@eylpartners.com