Introduction for Developing
Micro Quantum Random Number Generator
&
Applied Technologies

- 초소형 양자난수생성기의 개발과 응용기술 소개 -

EYL Inc.

2015.07

"EYL unfolds Cyber Society with no another me"

Startup Overview

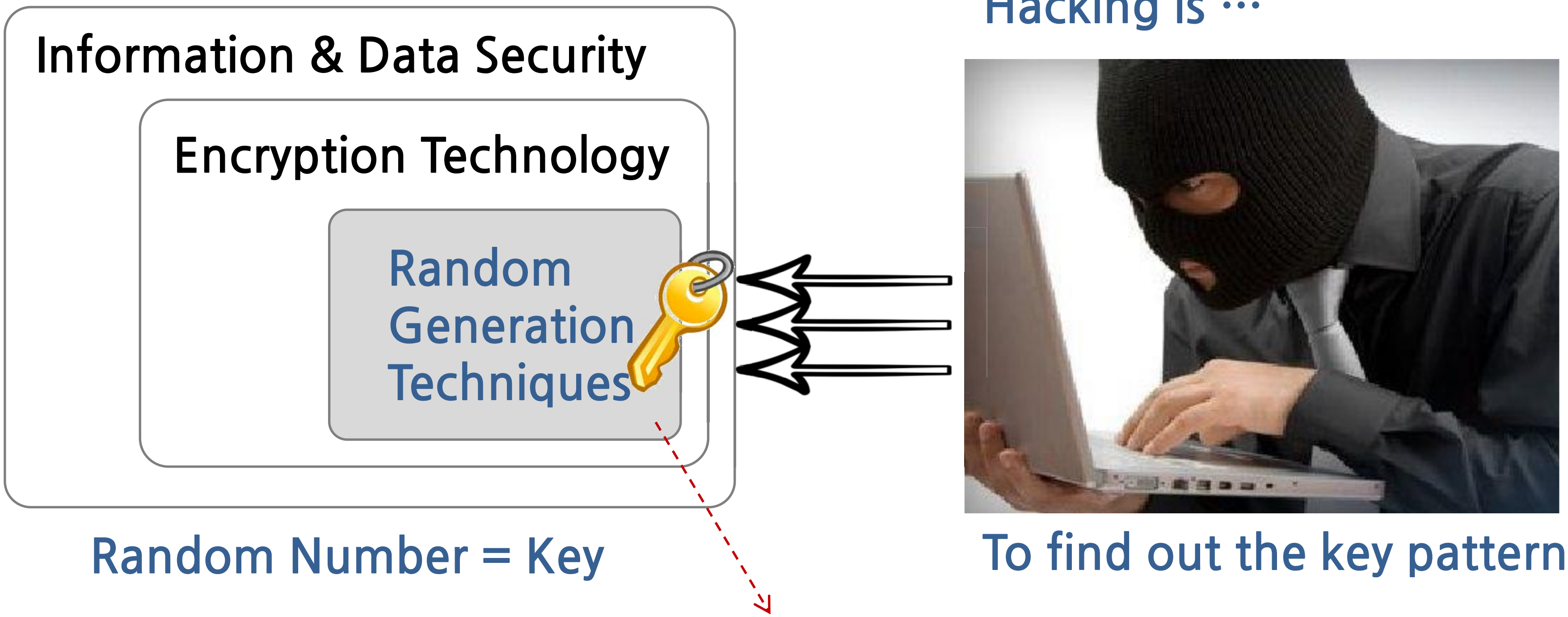
- Developing Micro QRNG & Applied Technologies
- From January, 2015
- Core Technology
  - ✓ Micro Quantum Random Number Generator - USB & Server
  - ✓ Applied Hardware - Micro QRNG Secured UMS, Serial Device
  - ✓ Authentication related Applications
- Selected as a Promising Startup in ‘K-Global IoT Startup Challenge 2015’
- www.eylpartners.com, www.facebook.com/eylkor

Randomness

- Critical element in designing a cryptographic algorithm
- Required to meet
  - ✓ Unpredictable
  - ✓ Unbiased
  - ✓ Uncorrelated

Limitations of Current Security System depending on Pseudo-Random Number

Hacking is …



Information & Data Security

Encryption Technology

Random Generation Techniques

Random Number = Key

To find out the key pattern

Pseudo-Random Number

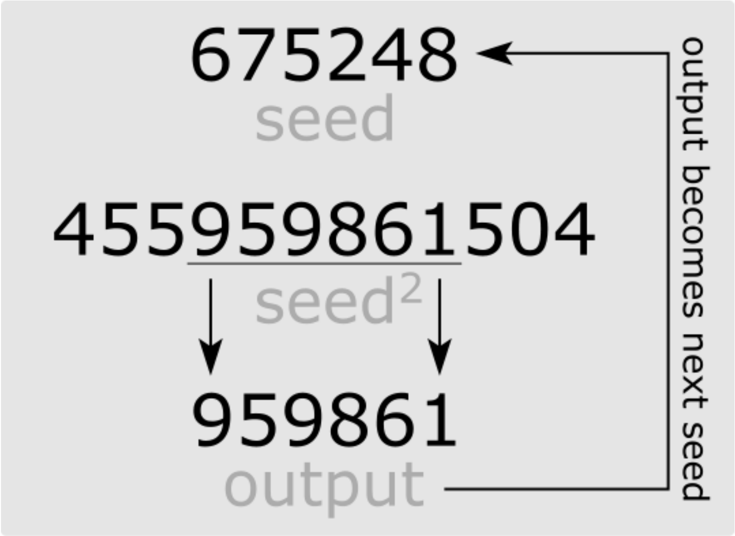
- With the development of computing capability, the random number generated by the mathematical algorithm, Pseudo-Random number, would not free from Hacking forever.

Pseudo-Random Number

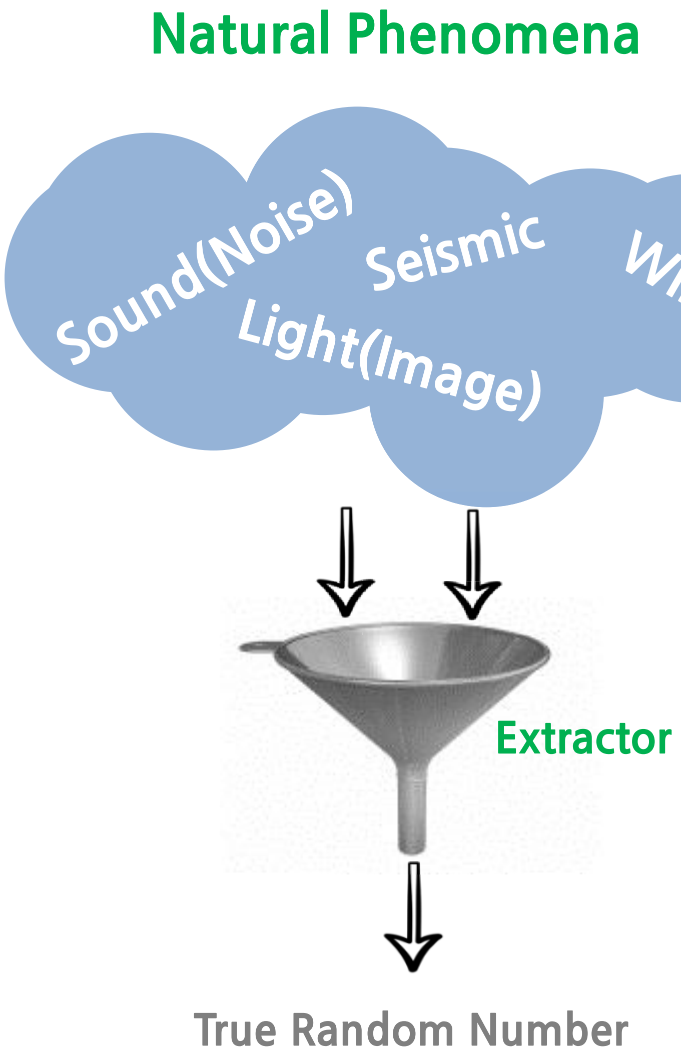
- Generated by mathematical algorithm
- Cannot be called ‘Random Number’ because…
  - ✓ Predictable

    if we know initial value(Seed) & Operating Condition
  - ✓ Correlated with previous value
- Computer is nothing to do with Random Number

example



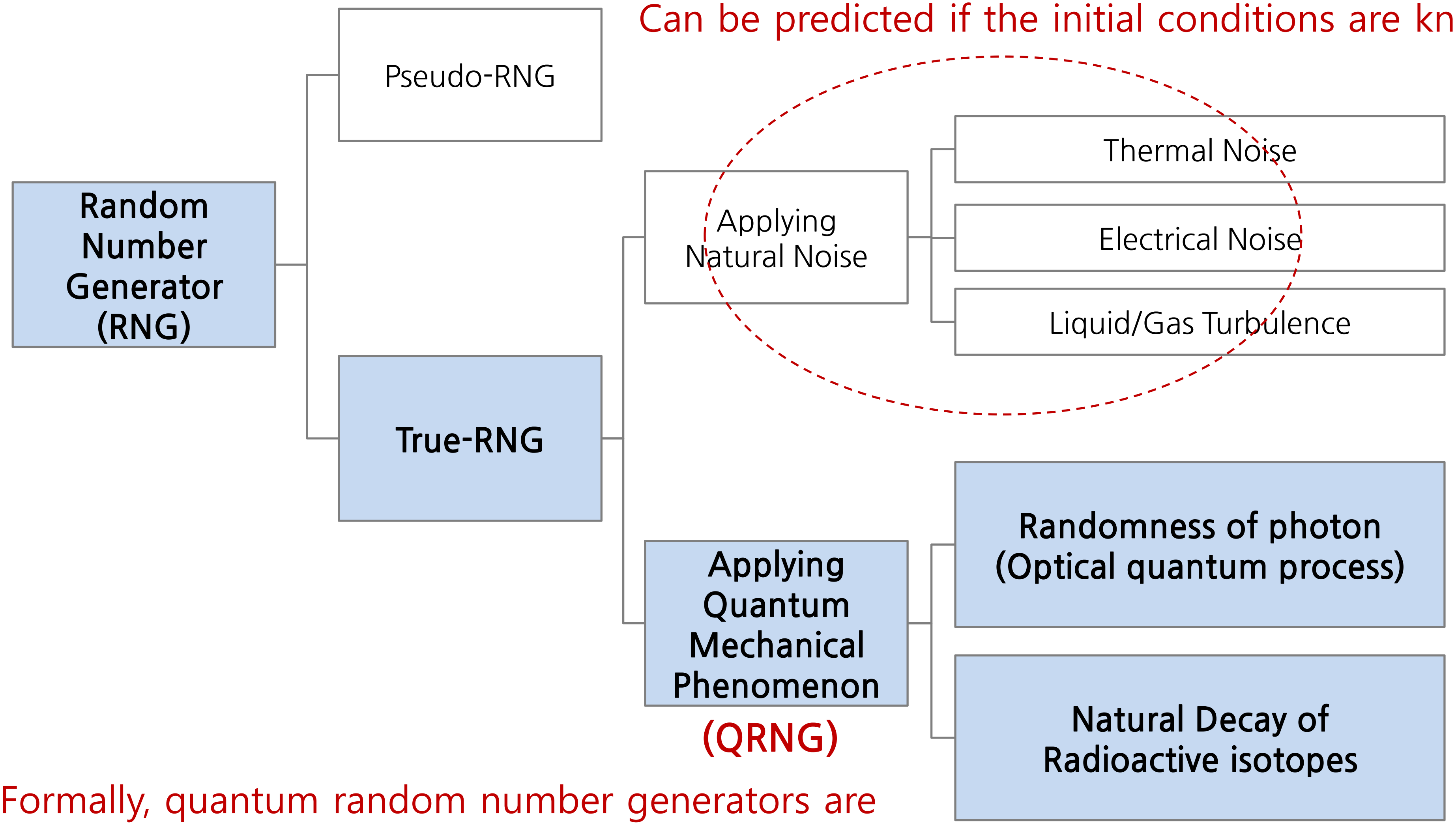
True Random Number



- Extracting Randomness from Nature
  → True Random Number
- No Pattern, Unpredictable
- Safe from hacking
- But …
  - ✓ Extractor Needed
  - ✓ Bulky, Very expensive
  - ✓ Limit to mount on IoT Device
  - ✓ Slow Speed
  - ✓ Biased Features
  - ✓ Lack of Reproducibility

Classification of the Random Number Generator

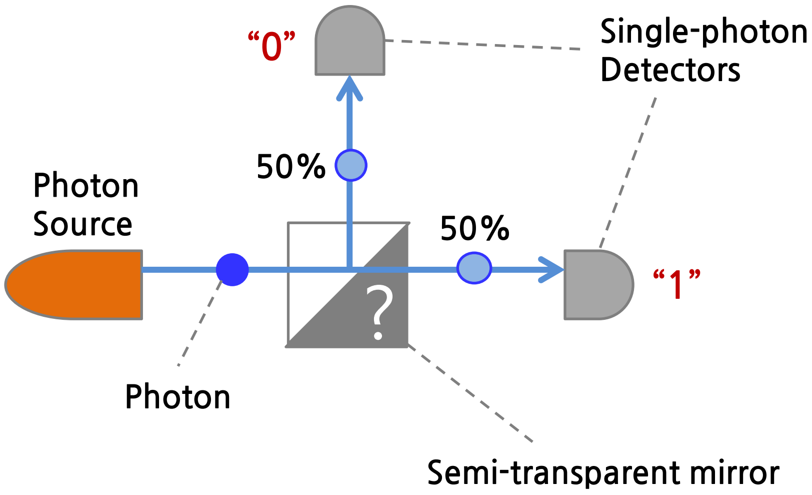
Classical physics is fundamentally deterministic.
Can be predicted if the initial conditions are known.


Random Number Generator (RNG)
Pseudo-RNG
True-RNG
Applying Natural Noise
Thermal Noise
Electrical Noise
Liquid/Gas Turbulence
Applying Quantum Mechanical Phenomenon
(QRNG)
Randomness of photon (Optical quantum process)
Natural Decay of Radioactive isotopes

Formally, quantum random number generators are only true random number generator

Recent Quantum Random Number Generator

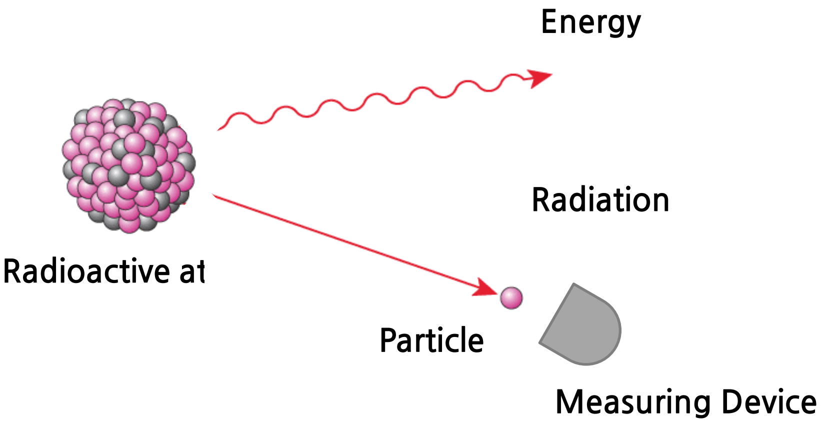
- Commercial optical type RNG



- ✓ Difficult to precisely balance
- ✓ Unbiasing Needed
- ✓ Ultra-Sensitive Detectors Needed
- ✓ Random Source Size :

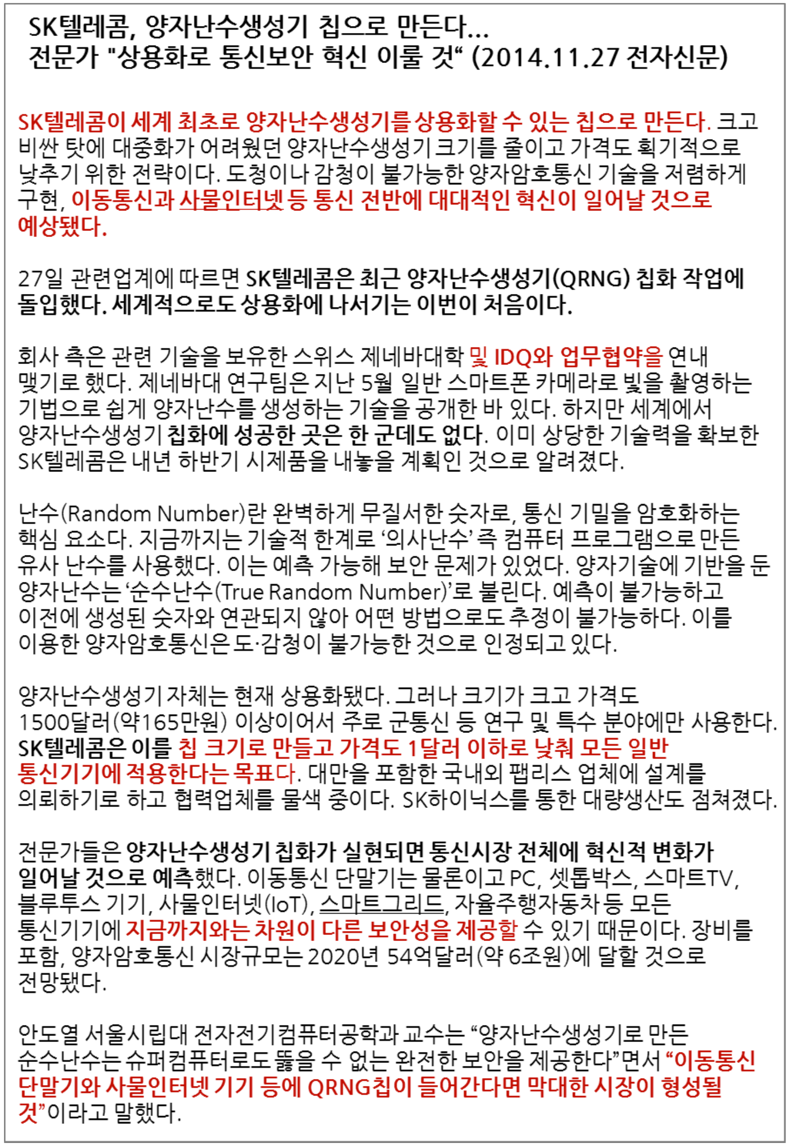
  51mm x 44mm x 17mm

- Observation type of the radioactive decay



- ✓ Produce numbers of Excellent Quality
- ✓ Not Commercialized
- ✓ Bulky
- ✓ May cause health concerns

Quantum Random Number Generator(QRNG) as a Chip?



SK텔레콤, 양자난수생성기 칩으로 만든다...
전문가 "상용화로 통신보안 혁신 이룰 것“ (2014.11.27 전자신문)

SK텔레콤이 세계 최초로 양자난수생성기를 상용화할 수 있는 칩으로 만든다. 크고 비싼 탓에 대중화가 어려웠던 양자난수생성기 크기를 줄이고 가격도 획기적으로 낮추기 위한 전략이다. 도청이나 감청이 불가능한 양자암호통신 기술을 저렴하게 구현, **이동통신과 사물인터넷 등 통신 전반에 대대적인 혁신이 일어날 것으로 예상됐다.**

27일 관련업계에 따르면 **SK텔레콤은 최근 양자난수생성기(QRNG) 칩화 작업에 돌입했다. 세계적으로도 상용화에 나서기는 이번이 처음이다.**

회사 측은 관련 기술을 보유한 스위스 제네바대학 **및 IDQ와 업무협약을** 연내 맺기로 했다. 제네바대 연구팀은 지난 5월 일반 스마트폰 카메라로 빛을 촬영하는 기법으로 쉽게 양자난수를 생성하는 기술을 공개한 바 있다. 하지만 세계에서 양자난수생성기 **칩화에 성공한 곳은 한 군데도 없다**. 이미 상당한 기술력을 확보한 SK텔레콤은 내년 하반기 시제품을 내놓을 계획인 것으로 알려졌다.

난수(Random Number)란 완벽하게 무질서한 숫자로, 통신 기밀을 암호화하는 핵심 요소다. 지금까지는 기술적 한계로 ‘의사난수’ 즉 컴퓨터 프로그램으로 만든 유사 난수를 사용했다. 이는 예측 가능해 보안 문제가 있었다. 양자기술에 기반을 둔 양자난수는 ‘순수난수(True Random Number)’로 불린다. 예측이 불가능하고 이전에 생성된 숫자와 연관되지 않아 어떤 방법으로도 추정이 불가능하다. 이를 이용한 양자암호통신은 도·감청이 불가능한 것으로 인정되고 있다.

양자난수생성기 자체는 현재 상용화됐다. 그러나 크기가 크고 가격도 1500달러(약165만원) 이상이어서 주로 군통신 등 연구 및 특수 분야에만 사용한다. **SK텔레콤은 이를 칩 크기로 만들고 가격도 1달러 이하로 낮춰 모든 일반 통신기기에 적용한다는 목표다**. 대만을 포함한 국내외 팹리스 업체에 설계를 의뢰하기로 하고 협력업체를 물색 중이다. SK하이닉스를 통한 대량생산도 점쳐졌다.

전문가들은 **양자난수생성기 칩화가 실현되면 통신시장 전체에 혁신적 변화가 일어날 것으로 예측**했다. 이동통신 단말기는 물론이고 PC, 셋톱박스, 스마트TV, 블루투스 기기, 사물인터넷(IoT), 스마트그리드, 자율주행자동차 등 모든 통신기기에 **지금까지와는 차원이 다른 보안성을 제공할** 수 있기 때문이다. 장비를 포함, 양자암호통신 시장규모는 2020년 54억달러(약 6조원)에 달할 것으로 전망됐다.

안도열 서울시립대 전자전기컴퓨터공학과 교수는 “양자난수생성기로 만든 순수난수는 슈퍼컴퓨터로도 뚫을 수 없는 완전한 보안을 제공한다”면서 **“이동통신 단말기와 사물인터넷 기기 등에 QRNG칩이 들어간다면 막대한 시장이 형성될 것”**이라고 말했다.

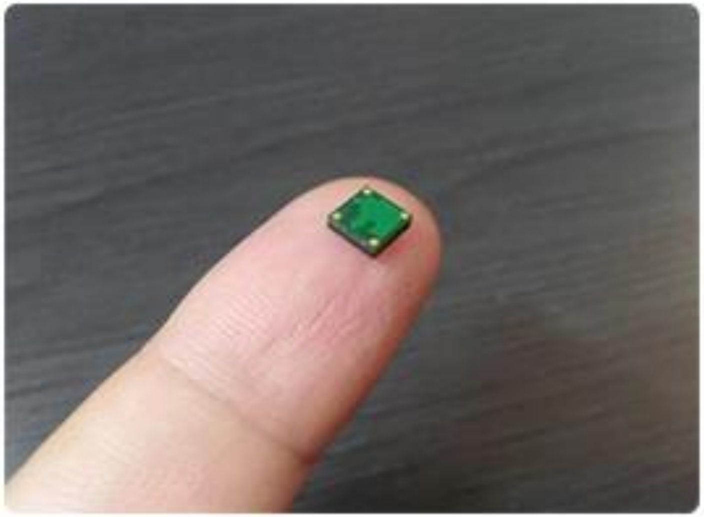
- Etnews(전자신문, Nov. 2014)
- SK Telecom will develop the first commercial Quantum Random Number Generator into Chip
- Business Agreement with Swiss Company & University
- Plan to make a dollar or less
- What will be happening the chip into IoT Devices …
  - ✓ Whole different security level
  - ✓ New security market

EYL’s Micro QRNG satisfies all of the conditions for IoT Devices

- Qualifications for IoT Device Components?

- Should be…

✓ Small	5mm x 5mm
✓ Cheap	To be $1 or less
✓ Unbiased	Satisfied
✓ Unpredictable	Satisfied
✓ Uncorrelated	Satisfied
✓ High Speed	4Mbps to 1Gbps (Developing, USB type)



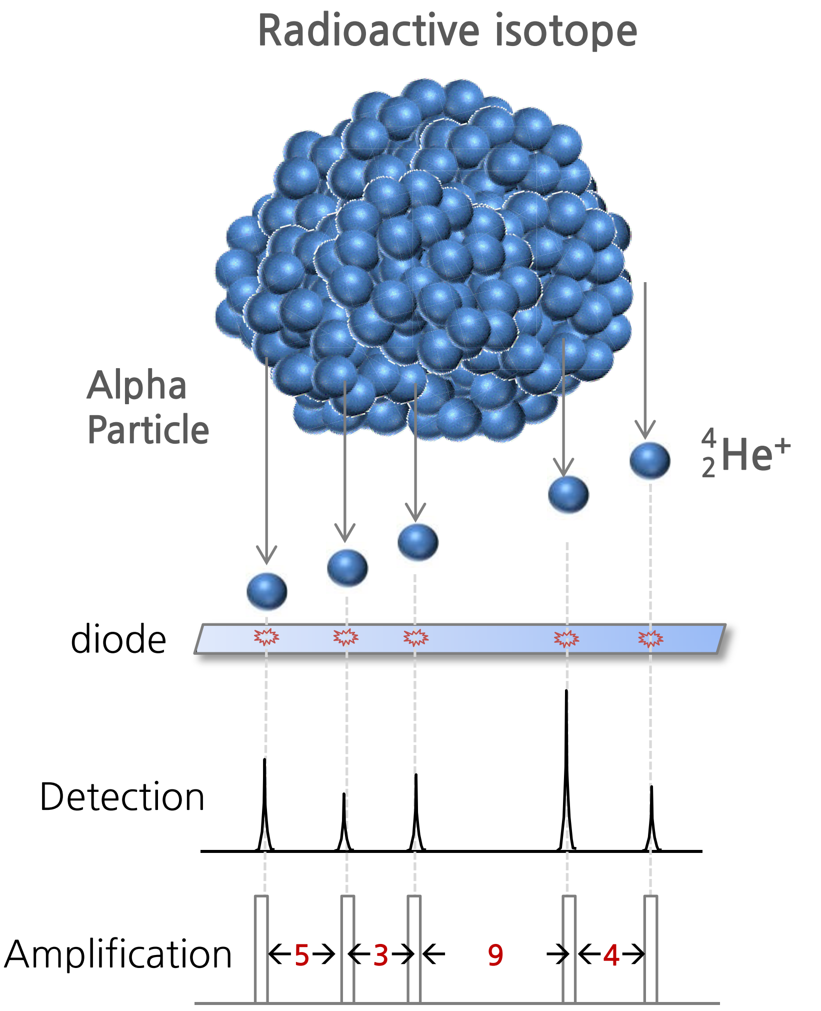
EYL’s Micro QRNG Chip

Compared to Commercialized optical QRNG Random Source

$\frac{1}{2180}$ Size, $\frac{1}{1000}$ Price

Smaller, Low power Thin Film Type is under development

Functionalizing Randomness of α Particles of the radioisotope



Measuring the time interval between pulse
Result : Random number 5, 3, 9, 4

- Functionalizing the release of α particle from the half-life of radioactive isotopes
- Complete Randomness assured by Uncertainty Principle of Quantum Mechanics
- Human Unpredictable
- Diode Collision → Pulse Generation
- Measuring the time interval between pulse
- Statistical correction is not necessary

(Very Large Energy, RN & Pulse is 1:1 correspondent)

Quality of Micro-QRNG

- **Passed all NIST* ST800-22 Verification Criteria : A Statistical Test Suite for Random Number Generators for Cryptographic Applications**

Test	Measurements	Proportion	Pass Condition (Proportion)	Results
The Frequency(Monobit) Test	0.57285	0.9900	>= 0.9	Pass
The Frequency within a Block	0.44469	0.9870	>= 0.9	Pass
The Runs Test	0.58108	0.9870	>= 0.9	Pass
Tests for the Longest-Run-of-ones in a block	0.44283	0.9820	>= 0.9	Pass
The Binary Matrix Rank Test	0.77919	0.9900	>= 0.9	Pass
The Discrete Fourier Transform Test	0.00224	0.9970	>= 0.9	Pass
The Non-overlapping Template Matching test	0.79627	0.9890	>= 0.9	Pass
The Overlapping Template Matching Test	0.38554	0.9940	>= 0.9	Pass
Maurer's"Universal Statistical" Test	0.26357	0.9860	>= 0.9	Pass
The Linear Complexity Test	0.91272	0.9870	>= 0.9	Pass
The Serial Test	0.48465	0.9910	>= 0.9	Pass
The Approximate Etropy Test	0.01779	0.9807	>= 0.9	Pass
The Cumulative Sums(Cusums) Test	0.41722	0.9870	>= 0.9	Pass
The Random Excursions Test	0.71327	0.9807	>= 0.9	Pass
The Random Excursions Variant Test	0.28531	0.9871	>= 0.9	Pass

* NIST: National Institute of Standards and Technology(US)

Safety of Micro-QRNG

- Alpha particles can be blocked by a piece of paper, even.
- Since alpha emitters being used in the Micro-QRNG is fully sealed, the radiation does not leak to the outside.
- Even if seal is broken, it is safe because radiation dosage is 10 μSV / year or less, that is under clearance level.
- Recycling
- Waste does not occur

Commonly applied in Smoke detectors

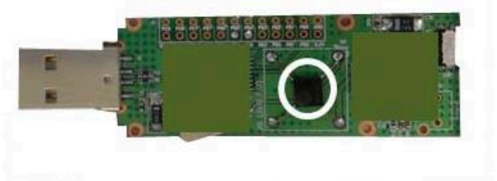
Micro-QRNG

If seal is broken,
1/100 of Public dose Limit

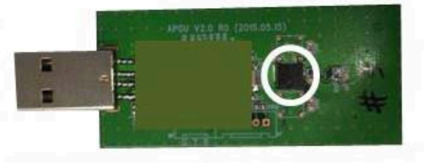
Various MQRNG and Applied Devices

White Circle : MQRNG Chip

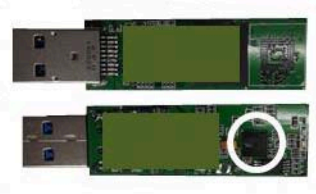
USB QRNG UTG491
(Liquid Type)



USB QRNG UTG251
(Disk Type)



USB QRNG UTG253



MQRNG Secured UMS
32G/64G

QRNG Server

- **USB Type QRNG**
  - Model No. UTG251~253, UTG491
  - Max. 20Kbps now
  - Target 1Gbps, under development
  - Windows/Linux
- **MQRNG Secured USB Mass Storage**
  - 32G/64G
  - Interface with Mobile Phone
- **Server Type QRNG**
  - Model No. STG25B01~03, STG25H01, STG25H02
  - Max. 100Kbps now
  - Target 4Gbps, under development
  - Windows Server 2008
- **PCI-E Type is under Development**

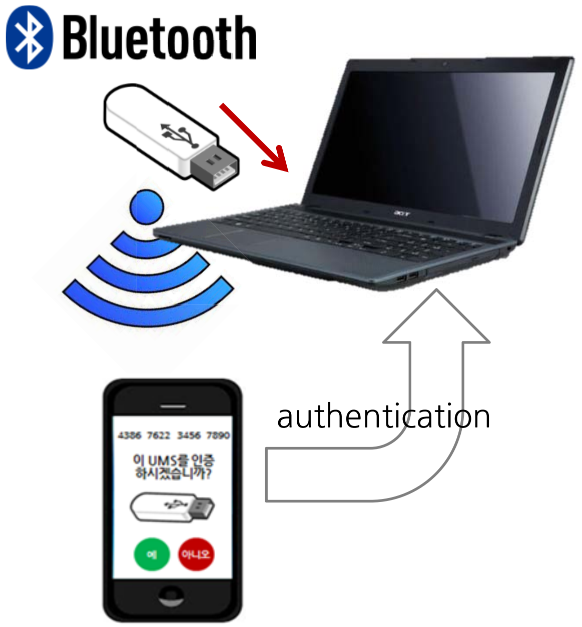
Various Quantum Devices under development for Authentication

- Micro-QRNG Secured USB Mass Storage 16G/32G
  - By Mobile Authentication

- Micro-QRNG Secured Personal Authentication Device & dongle
  - USB Type, Serial Type
  - Korea Patent No.1244853

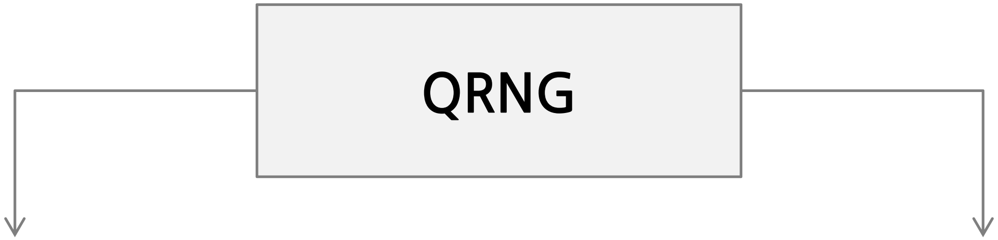
- Micro-QRNG Secured Door Lock
  - By Mobile Authentication

- Micro-QRNG Immobilizer
  - Korea Patent No.1523760



Encryption & Authentication applied to Communication and IoT Devices

- Micro-QRNG provides Encryption & Authentication key with no Algorithm subject to Hacking


QRNG

⦿ Symmetric key Cypher Algorithm

⦿ Public key Cryptography

⦿ Block Cipher Mode

⦿ Initial Vector Generation

⦿ Nonce Generation

⦿ Salt Generation

⦿ Padding Generation

⦿ OTP(One Time Password)

⦿ CAPTCHA

⦿ Message Authentication Code

⦿ Digital Signature Key

⦿ Mobile Authentication Number

⦿ Coupon Number

⦿ Online/Mobile Game

⦿ Social Research, Drawing, Lottery, etc.

QRNG-Applied Solutions

- RoBAC 2.0 : System Log-In Security Technology
  - No password, no hacking
  - Linkage applied to system log-in or particular functionalities
  - Easy One-Touch
  - Applied to Log-in by employee and contractor
- Appraiser 1.5 : Applied to material flow and supply chain for Fake Prevention
  - Smart phone touch on product or certificates for genuine identification
  - Every time at authentication, compare with source random number
  - Generate new random number into phone & NFC tag of product
  - Only one and unique product, big data application using product touch by product. Build up Brand Image
- Acloid 1.5 : Applied to ID & Credit Card Authentication
  - Store MQRNG random number in card at new card issue
  - At mobile authentication, compare with unique source RN stored in Server
  - Generate new RN into the card for next authentication
- R&D in progress
  - FinTech
  - Authentication Solutions for Smart Home & Connected Car
  - Smaller, low power thin film Micro-QRNG

“EYL unfolds Cyber Society with no another me”

또 다른 내가 없는 안전한 사이버 세상, EYL이 만들어 갑니다

Thank you!

Contact : JH Baik / +82.10.3168.1418 / mqrng@eylpartners.com