초소형 양자난수생성기의 개발과 응용기술 소개

Introduction for Developing
Micro Quantum Random Number Generator
&
Applied Technologies

EYL Inc.

2015.09

"EYL unfolds Cyber Society with no another me"

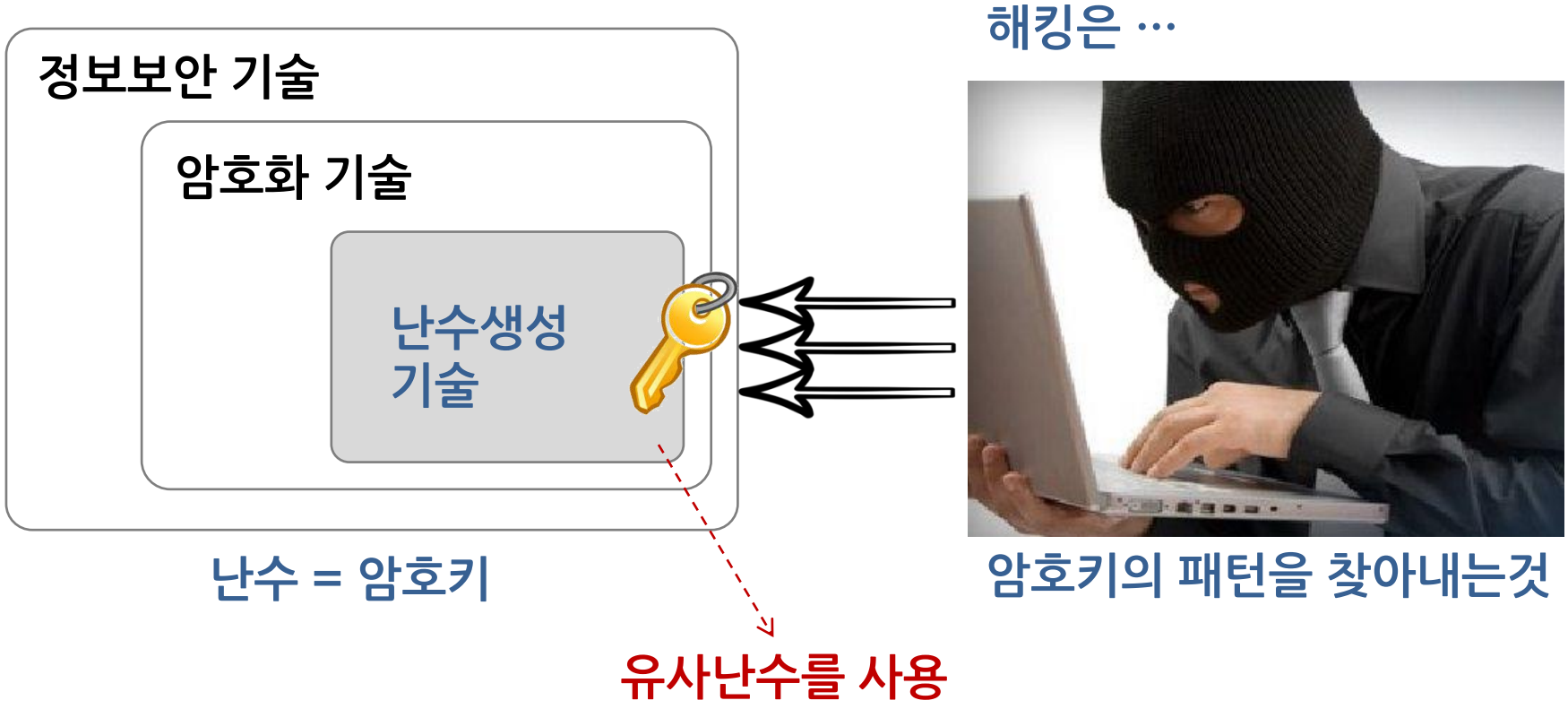
Startup Overview

- 초소형 양자난수 생성기의 개발과 응용기술
- 2015년 1월 창립
- 인터넷진흥원 주관 'K-Global IoT Startup Challenge 2015' 유망 스타트업으로 선정
- www.eylpartners.com, www.facebook.com/eylkor

난수란?

- 암호화 시스템을 구성하는데 필수적인 요소
- 난수의 조건
  - ✓ 예측 불가능성(Unpredictable)
  - ✓ 무편향성(Unbiased)
  - ✓ 숫자간 무관성(Uncorrelated)

유사난수를 사용하는 현재의 보안 시스템 한계



- 컴퓨팅 기술이 발전하면서 수학적인 알고리즘으로 만들어 내는 유사난수를 사용한 암호화 기술은 해킹에 노출

유사난수

- 풀어내는데 엄청난 시간이 걸릴 것이라는 가정 하에 수학적인 알고리즘으로 만든 계산 결과
- 실질적인 '난수'가 아닌 이유는…

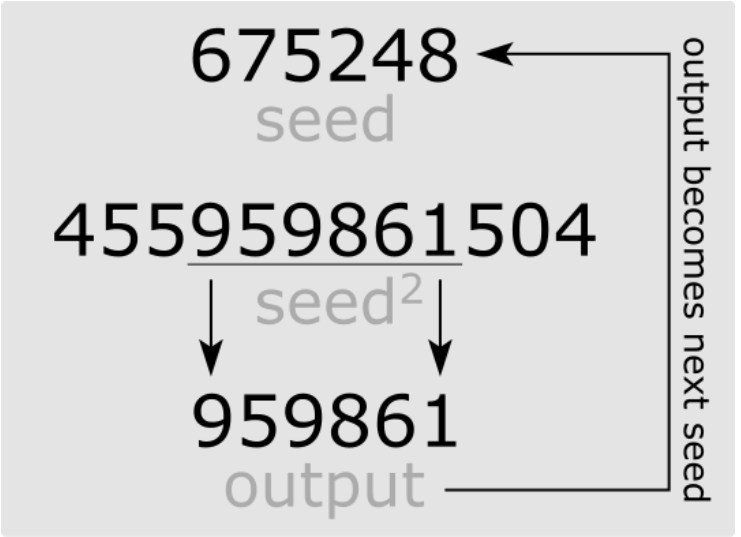
  ▶ 예측 가능

  초기값(seed)과 동작상태를 알 경우

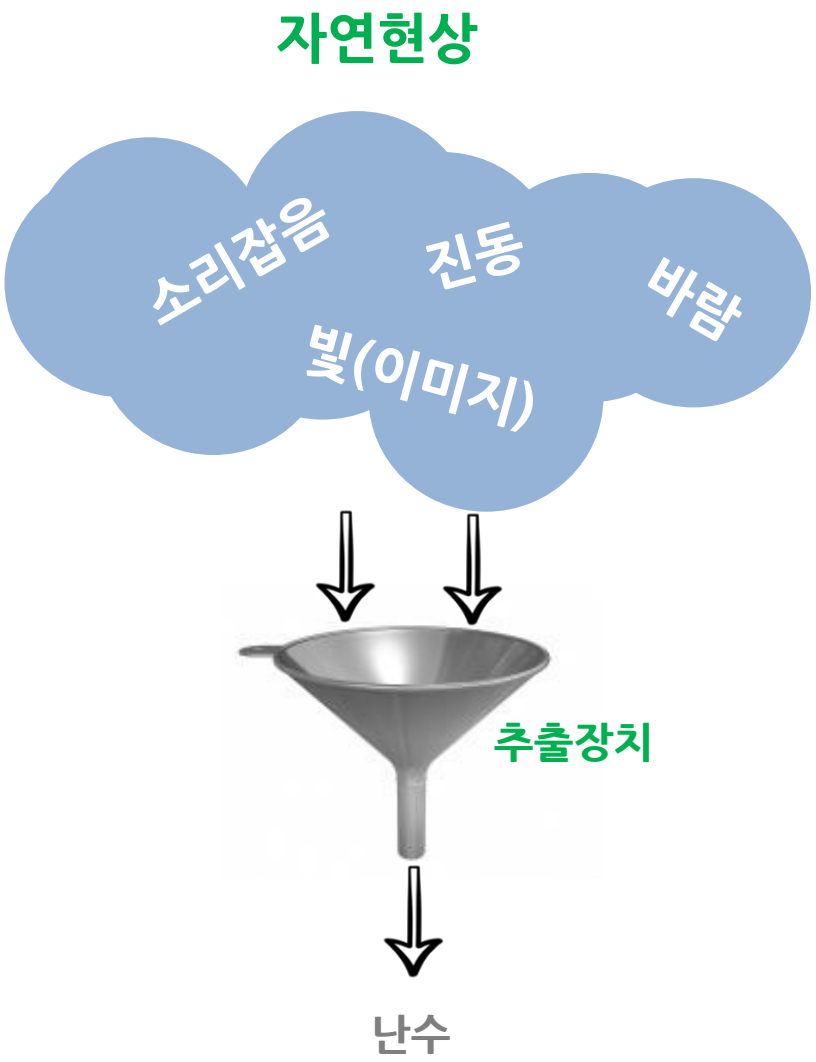
  ▶ 상호 연관성

  앞에 발생한 숫자와 연관 됨
- 따라서 컴퓨터는 난수를 만들어 낼 수 없는 장비임

example

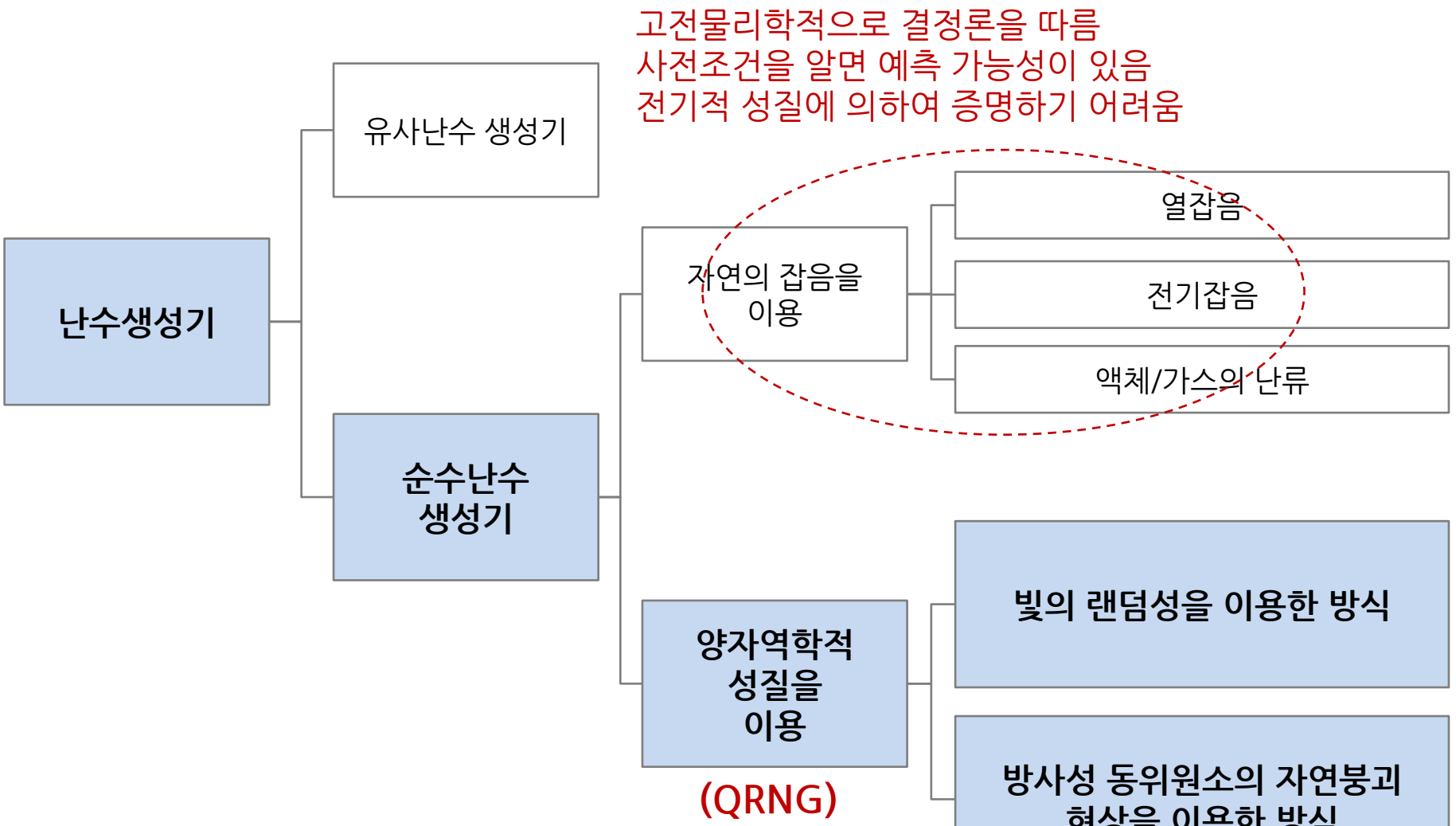


진정난수



- 자연현상의 무작위성에서 난수를 추출
  → 진정난수/자연난수/순수난수라고 함
- 패턴 없음, 예측이 불가능함
- 해킹으로부터 안전
- 하지만…
  - ✓ 추출장치 필요
  - ✓ **크기가 크고 매우 비쌈**
  - ✓ IoT Device에 적용불가능
  - ✓ **속도가 느림**
  - ✓ **편향성이 심함**
  - ✓ 재생성이 어려움

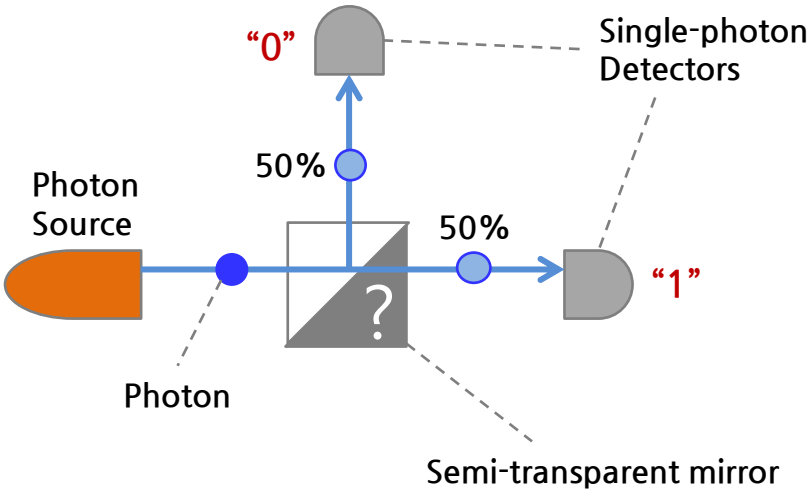
난수생성기의 분류



공식적으로는 양자난수생성기가 유일한 난수생성기임

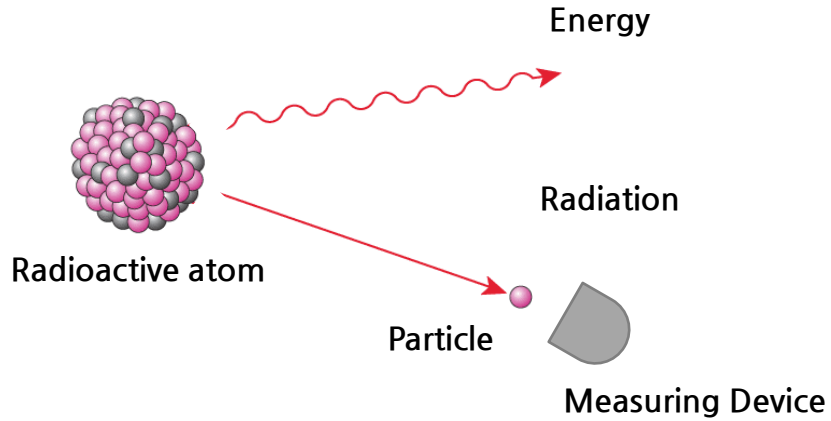
최근 양자난수생성기 기술동향

- 상용화 된 빛(광자의 랜덤성)을 이용한 방식



- ✓ 정확하게 50%투과 mirror 제작은 불가능 → 편향성 보정 필요
- ✓ 초고감도 센서가 필요함
- ✓ 크고 비쌈 (16Mbps, 300만원선)

- 방사성 동위원소를 이용한 방식



- ✓ 아주 좋은 품질의 난수를 생성함
- ✓ 크기가 크고 비쌈
- ✓ 인체에 해로움
- ✓ 상용화 되지 못함

양자난수생성기를 칩으로 만든다?

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.

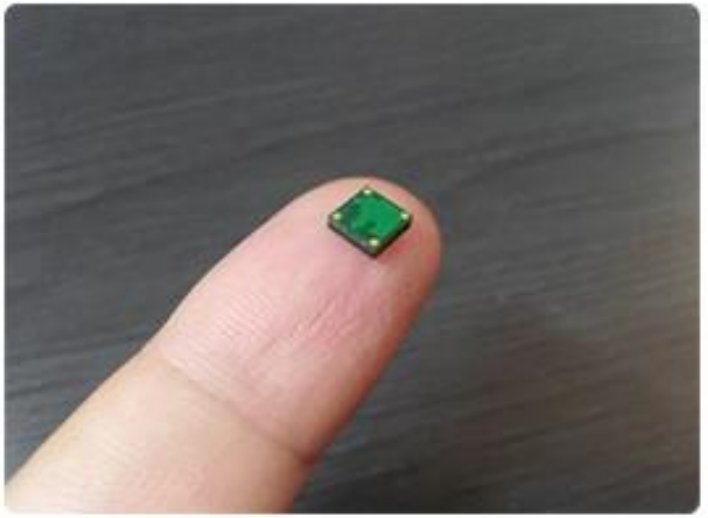
안도열 서울시립대 전자전기컴퓨터공학과 교수는 "양자난수생성기로 만든 순수난수는 슈퍼컴퓨터로도 뚫을 수 없는 완전한 보안을 제공한다"면서 **"이동통신 단말기와 사물인터넷 기기 등에 QRNG칩이 들어간다면 막대한 시장이 형성될 것"**이라고 말했다.

- 출처: 전자신문(2014.11.27)
- SK Telecom 이 세계최초로 양자난수생성기를 칩으로 만든다
- 현재 특수 보안을 요하는 군사용으로만 사용
- 스위스의 대학 및 기업과 협약
- 1달러 이하로 제작
- 일반적인 IoT 기기에 들어갈 경우
  - ✓ 차원이 다른 보안성 제공
  - ✓ 막대한 시장 형성

EYL의 Micro QRNG 는 IoT 기기에 장착 될 수 있는 조건을 충족

- IoT 기기에 장착 할 수 있는 조건은?

- 다음의 조건을 충족해야 함
  - ✓ 작고 — 5mm x 5mm
  - ✓ 싸고 — To be $1 or less
  - ✓ 무편향성 — Satisfied
  - ✓ 예측불가능성 — Satisfied
  - ✓ 무연관성 — Satisfied
  - ✓ 빠른속도 — 4Mbps to 1Gbps (Developing, USB type)



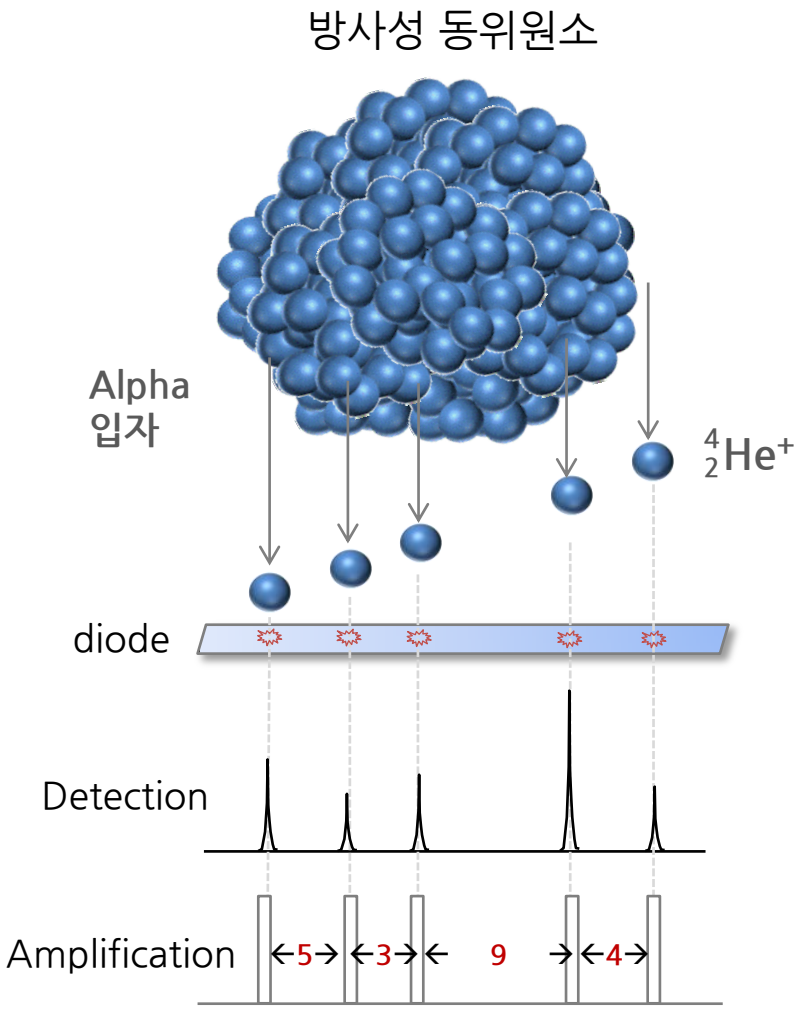
EYL's Micro QRNG Chip

상용화 된 광학식 양자난수생성기 랜덤 소스 대비

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

- 현재 더 작고, 더 얇은 박막형태의 Micro QRNG 개발 중
- 양자펄스발생원 + CPU + 암호모듈이 탑재 된 초소형(3mm x 3mm), 저가형 SoC 개발 중

Micro QRNG의 원리



펄스간의 시간간격 측정 : Random number 5, 3, 9, 4

- 방사성 동위원소에서 반감기 동안 방출하는 알파입자를 이용
- 양자역학적으로 불확정성을 따르므로 완전한 난수성을 가짐
- 인간이 예측할 수 없는 난수를 만들어 냄
- 알파입자 → 다이오드 충돌 → 펄스 생성
- 펄스간의 시간간격을 측정하여 난수 생성

EYL Micro-QRNG 난수의 품질

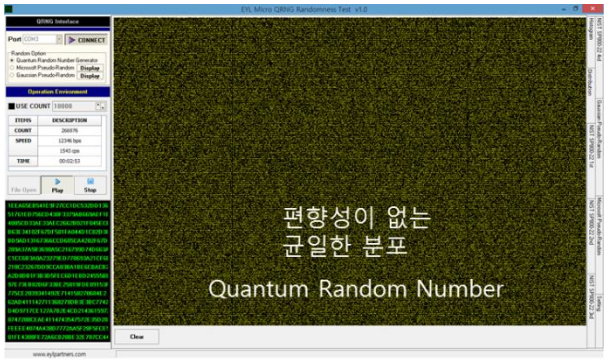
- 모든 NIST* ST800-22 Verification Criteria 통과: A Statistical Test Suite for Random Number Generators for Cryptographic Applications

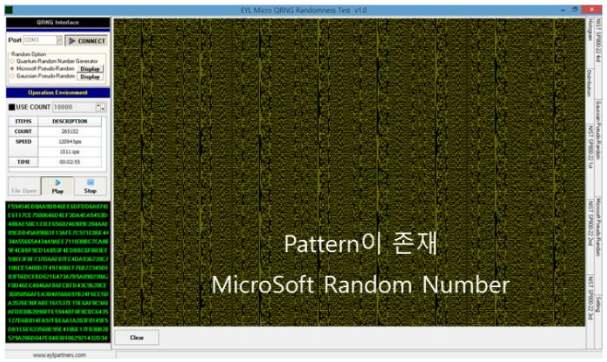
Test	Measurements	Proportion	Pass Condition (Proportion)	Results
The Frequency(Monobit) Test	0.57285	0.9900	>= 0.9	Pass
The Frequency within a Block	0.44469	0.9870	>= 0.9	Pass
The Runs Test	0.58108	0.9870	>= 0.9	Pass
Tests for the Longest-Run-of-ones in a block	0.44283	0.9820	>= 0.9	Pass
The Binary Matrix 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

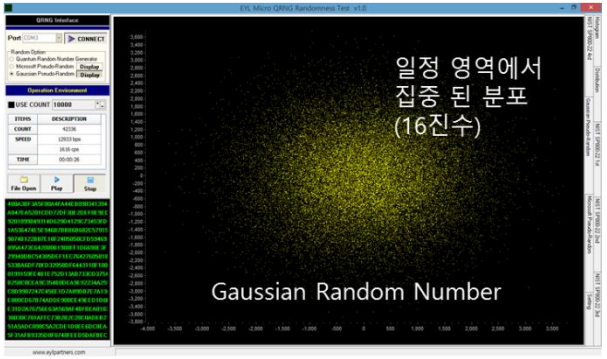
* NIST: National Institute of Standards and Technology(US)

EYL Micro-QRNG 난수의 품질

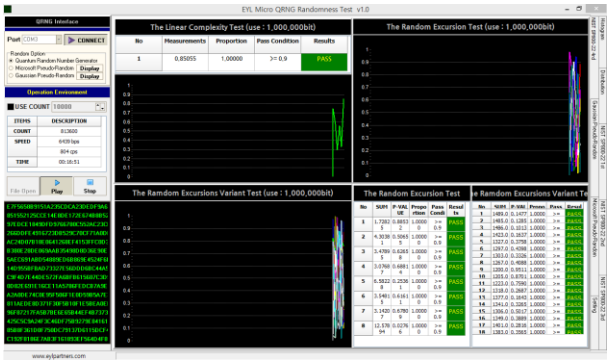
- Micro-QRNG의 난수와 Microsoft 및 Gaussian 유사난수의 발생분포 비교







- Micro-QRNG의 실시간 NIST 난수 품질 검증항목 테스트(모든 항목 Pass)



Micro-QRNG의 안전성

- 알파입자는 종이 한 장으로 막을 수 있음
- 상용화 된 화재감지기에 사용되는 알파 입자 방출체의 1/80 크기로 극미량 사용
- 밀봉된 상태에서는 법적으로도 방사능 물질로 취급되지 않음
- 알파입자 방출체는 완전히 밀봉되어 칩 밖으로 방사능이 나오지 않음
- 파손될 경우에도 방사선 노출량이 10 μSV / year 이하

Commonly applied in
Smoke detectors

Micro-QRNG

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

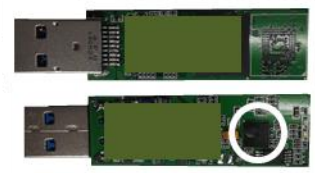
Micro-QRNG를 활용한 다양한 난수생성 기기

흰색 원 : 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**

Micro-QRNG를 활용한 다양한 인증기기

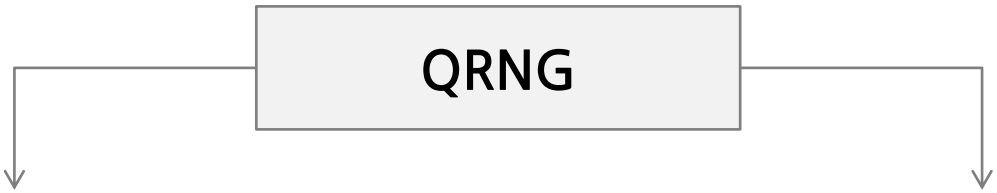
- Micro-QRNG를 적용한
  개인 인증 기기 및 USB동글
  - USB Type, Serial Type
  - 한국특허 No.1244853

- Micro-QRNG를 적용한 도어락
  - 핸드폰 인증 적용

- Micro-QRNG Immobilizer
  - 한국특허 No.1523760

암호화 통신 및 IoT 사물간 통신에 암호화/인증 키 제공

- Micro-QRNG는 안전한 암호화 및 인증키를 사용자 요구에 맞도록 제공



- ⦿ 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.

- 현재 암호 전문업체인 D사와 함께 국정원 검증필 암호모듈 개발 진행 중 (2016년 3월 인증 완료 예정)

기타 Micro-QRNG 적용 솔루션

- RoBAC 2.0 : 2Channel 로그인 인증 시스템
  - 패스워드를 없애고 일회성 인증번호를 사용자에게 전달
  - 한수원 해킹 방식을 방지
  - 원터치 방식의 로그인
- Appraiser 1.5 : 진품판정 솔루션
  - 주류, 명품 등 위조품이 많은 제품 생산 시 NFC 태그에 난수를 적용하여 삽입
  - 핸드폰 터치로 진품인지 위조품인지를 실시간 인증
  - 인증하는 순간 IOTP(Invisible One Time Password)를 제조사에서 생성하여 다시 NFC 태그에 기록
  - 해당 난수를 가지는 유일한 1개의 제품만 존재
  - 수집 된 사용자 단말 정보를 빅데이터로 이용하여 마케팅에 활용
- Acloid 1.5 : 신분증, 크레디트카드 위/변조 방지 솔루션
  - 신분증, 크레이트카드 발급 시 난수를 적용하여 삽입
  - 리더기 및 핸드폰 터치로 위조 카드인지를 실시간 인증
  - 인증 순간 IOTP를 생성하여 다시 새로운 난수를 기록
  - 해당 난수를 가지는 유일한 1개의 카드만 존재
  - 조회하는 인가자의 권한별로 차별화 된 정보 제공
- R&D 진행
  - 핀테크
  - Smart Home & Connected Car
  - 작고 얇은(박막형) Micro-QRNG

국산 '초소형 양자난수생성기' 나온다

이와이엘 '마이크로 QRNG' 개발
5×5㎜ 크기에 가격도 1달러 미만
스마트홈 IoT 보안 등에 활용 가능

국내 스타트업이 초소형 양자난수생성기 개발에 성공했다. 사물인터넷(IoT) 기기를 보호하는 새로운 방법이 될 전망이다.

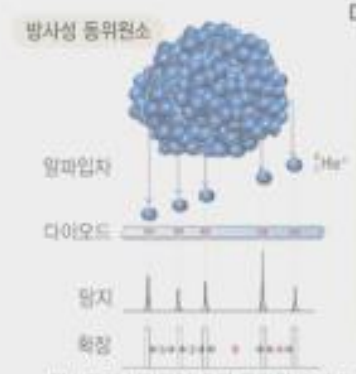
이와이엘(대표 우찬호 www.eylpartners.com)은 방사성동위원소 반감기를 이용해 초소형 양자난수생성기 '마이크로 QRNG'를 개발했다. 컴퓨팅 기술이 발전하면서 수학 알고리즘으로 만든 유사난수는 해킹 위험이 높아졌다. 공격자는 컴퓨팅 파워를 높여 숫자 간 상호 연관성을 분석해 유사난수를 푼다.

하드웨어 난수생성기는 자연에서 발생하는 노이즈나 양자역학적 성질을 이용한 난수발생 장치다.

난수는 일정한 규칙이 없어 예측이 어렵다. 양자난수생성기는 알고리즘이 없어 사용자가 원하는 안전한 암호화와 인증키를 제공한다. 기존 양자난수생성기는 규모가 큰 장치가 필요한 데다 고가여서 상용화가 쉽지 않다.

이와이엘은 방사성 동위원소가 자연붕괴하는 방식을 활용해 양자난수생성기를 개발했다. 약 400년에 달하는 방사성 동위원소 반감기에 방출하는 알파입자를 이용한다. 알파입자를 다이오드에 충돌시켜 펄스를 생성한다. 펄스 간 시간간격을 측정해 난수를 만든다.

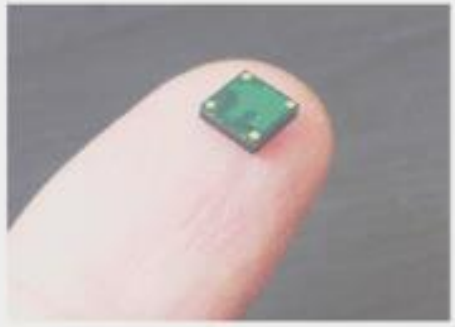
이와이엘 양자난수생성기는 5×5㎜ 크기로 여성 새끼 손가락 손톱보다 작고 가벼운 데다 가격도 1달러 미만이다. 양자난수생성기에 쓰는 알파입자는 이미 상용화된 화재감지기에 쓰는 알파입자의 80분에 1에 지나지 않는다.



펄스간의 시간간격 측정:무작위 숫자 5, 3, 9, 4

마이크로 QRNG의 원리

- 방사성 동위원소에서 반감기 동안 방출하는 알파입자를 이용
- 양자역학적으로 불확정성을 따르므로 완전한 난수성을 가짐
- 인간이 예측할 수 없는 난수를 만들어 냄
- 알파입자→다이오드 충돌→펄스 생성
- 펄스간의 시간간격을 측정하여 난수 생성


이와이엘이 개발한 양자난수생성기 '마이크로 QRNG'

마이크로 QRNG에서 나온 난수는 미국 표준협회(NIST) ST800-22 인증을 통과하며 품질도 인정받았다.

크기가 작아 다양한 분야에 활용이 가능하다. 신분증이나 신용카드에 마이크로 QRNG칩을 넣어 발급한다. 해당 난수를 가진 신분증은 유일해 리더나 스마트폰으로 스캔하면 위조 여부를 실시간으로 알 수 있다.

주류나 명품 등 위조품이 많은 제품을 생산할 때 NFC 태그에 난수를 적용하면 진품을 바로 판정할 수 있다.

핀테크에도 활용된다. 스마트폰 등 개인 기기와 서버에 각각 마이크로 QRNG를 적용해 난수를 주고받아 인증한다. 이외에 이모빌라이저 등 차량보안시스템과 스마트 도어록, 스마트홈 IoT 등에 적용할 수 있다.

우찬호 이와이엘 대표는 "마이크로 QRNG는 외부 온도와 압력, 전자파에 전혀 영향을 받지 않고 인체에 무해하다"며 "방사체를 액체로 만든 후 증발시켜 얇은 막으로 만들면 시스템온칩(SoC)으로 제조가 가능해 지금보다 더 얇고 작게 만들 수 있다"고 설명했다.

이와이엘은 한국인터넷진흥원이 주관한 'K글로벌 IoT스타트업 챌린지 2015'에서 유망 기업으로 선정됐다.

김인순기자 insoon@etnews.com

“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