양자난수생성기술

(Quantum RNG)

Korea Institute of Science and Technology

2017. 09.

Random Number Generator Overview

❒ 난수생성기(Random Number Generator, RNG)

- 난수생성기술은 암호와 같은 보안 시스템을 비롯해 통신, 전자금융거래, 웹 서비스, 게임 등 **정보통신기술(ICT) 전 분야에 기본으로 쓰이는 필수적인 보안 기술임**
- 현재까지 개발된 기술들 중 **유사난수(Pseudo Random Number)를 사용한 암호화 기술은 해킹에 노출되어 보안성 문제가 심각해져 양자역학적 성질을 이용하여 난수를 형성하는 양자난수발생기술에 대한 기대치가 높음**

❒ RNG 기술분류

- Random Number Generator
  - Pseudo Random Number Generator
    · Algorithm
    - 높은 비트율, 바이어스되지 않은 출력, 비용 효율, 및 실행의 용이성
    - 특정패턴 존재
    - **해킹 가능**
  - True Random Number
    · Physical Process
    - 물리적 무질서 상태 이용(PRNG)
      · 열 잡음, 무질서 레이저, 회로 잡음, 광 잡음 등
    - 양자역학적 성질 이용(QRNG)
      · 방사성 동위원소
      · 빛의 랜덤성 등.

패턴이 없고, 예측이 불가능하여 해킹 불가능

Market Forecast

❒ Random Number Generator 적용 시장예 (양자암호통신시장)

[Global 시장]

[국내 시장]

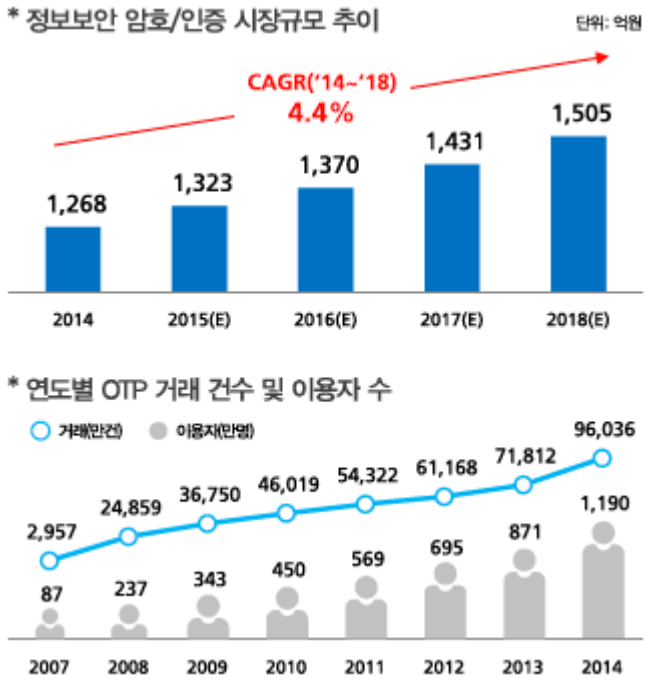
출처 : 글로벌 시장은 Market Research Media(2016-2020), 2020년 이후 및 국내시장 규모는 IITP 추정

- 전세계 양자암호통신 시장은 **연평균 22.5%의 성장률**을 보이며, **2025년에 26조 9000억원 규모**에 이를 것으로 전망

- 국내 양자암호통신 시장은 **연평균 84.9%의 성장률**을 보이며, **2025년에 1조 4000억원 규모**에 이를 것으로 전망

Market Forecast

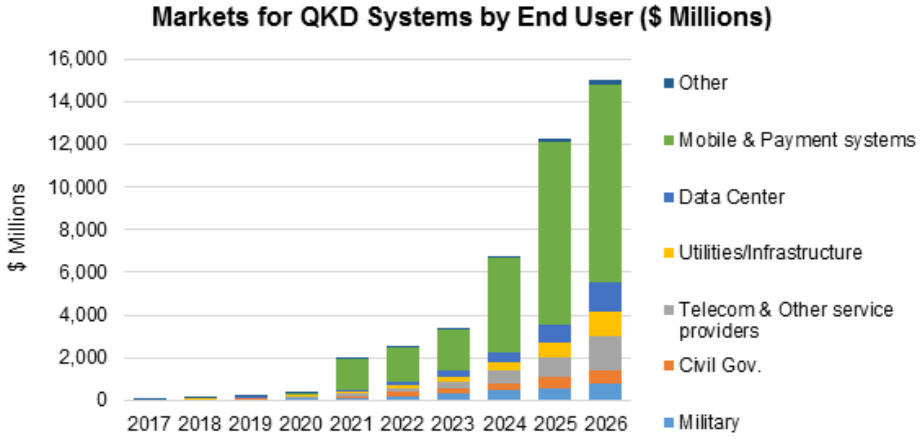
❒ 정보보안 시장 규모 추이 및 OTP이용자 수



출처 : 미래테크놀로지

- **2018년**의 정보보안 시장의 규모는 2014년 대비 CAGR이 4.4% 증가한 **1,505억원으로 예상**
- 연도별 OTP거래 건수 및 이용자 수는 **인증 및 보안 수요 증가로 계속적으로 증가**하고 있음

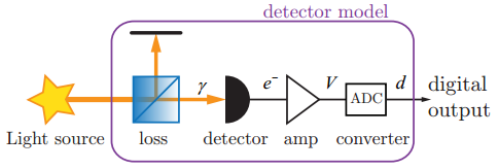
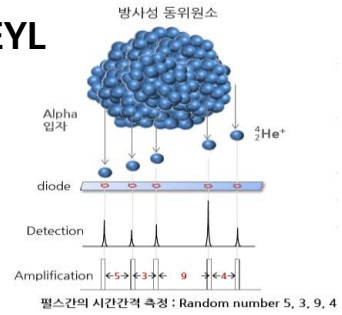
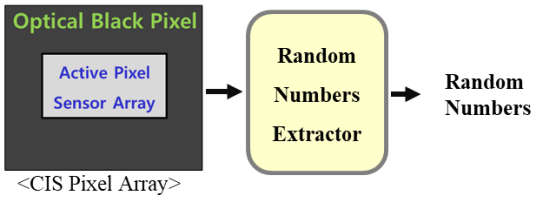
❒ 양자 키 분배 (QKD) 시스템 시장



출처 : Communications Industry Researchers, Inc.

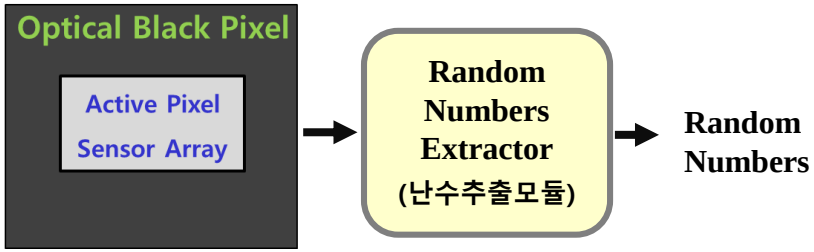
- **양자 키 분배 (QKD) 시스템 시장**이 **2022년까지 25 억 달러로 성장**할 것으로 예상
- QKD시스템 시장에tj **모바일 및 지불 시스템 분야는 큰 비중을 차지하며 성장**할 것으로 전망

Quantum RNG technology

	스위스 IDQuantique	한국 EYL	KIST
			 <CIS Pixel Array>
원리	• 광원(LED)을 제공하여 CIS의 Active pixel영역에서 생성되는 **Photon shot 노이즈 이용**	• 방사성동위원소에서 반감기 동안 방출하는 알파입자를 이용	• **광원없이** CIS의 black pixel영역에서 생성되는 **Dark shot 노이즈 이용**
장단점	• **별도의 하드웨어(광원) 필요** • 빛을 안정화시키기 위한 복잡한 피드백 하드웨어 및 전체 픽셀에서 빛을 일정하게 하기 위한 광학 장치가 요구되어 모바일 어플리케이션에 적용하기에는 제한적	• **별도의 칩으로 제작필요** • 복잡한 하드웨어가 추가되어야 함 모바일 어플리케이션에 부적합	• **기존 CIS 이미지센서에 하드웨어 없이 소프트웨어적으로 양자난수발생 가능** • **다크샷 노이즈는 포아송 분포로 양자난수 생성이 가능함이 입증**
성능	• **Mbit**	• 4Mbit to 1Gbit (Developing, USB type)	• 6.8 Mbit(1M Pixel) • 이미지센서 사양에 따라 조절 가능
기타	• SKT로 기술이전		• **NIST test 검증완료**

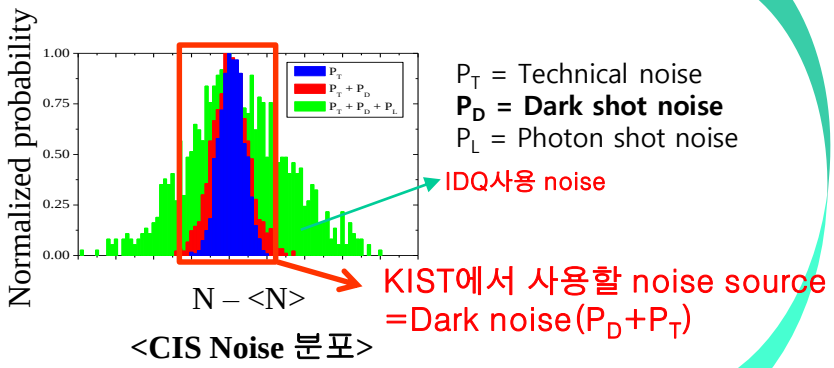
KIST Quantum RNG (1)

❒ KIST QRNG Summary



<CIS Pixel Array>

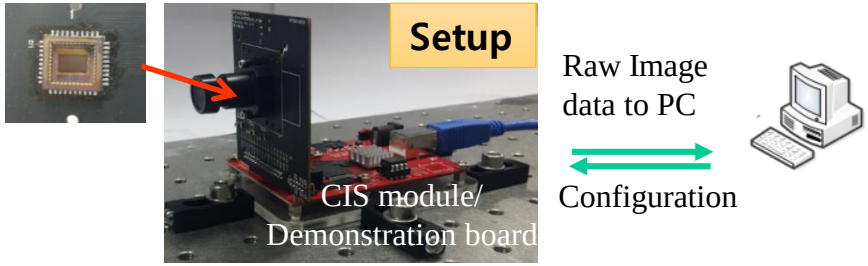
- 광원 없이 CIS 이미지센서의 픽셀 어레이 중 Optical black pixel 영역에서 생성되는 Dark shot noise를 추출하여 양자난수 생성



<CIS Noise 분포>

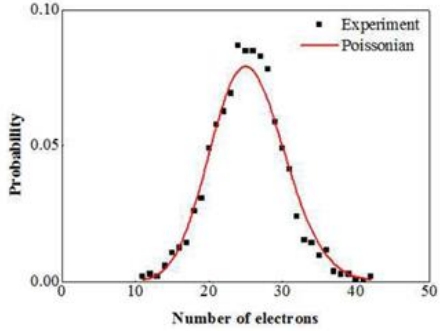
- Dark noise(P_D+P_T)를 후처리를 통해 Technical noise를 제거한 후 Dark shot noise 추출

❒ Experiments



- CIS에 **Dark shot noise**만 추출하기 위해 **Cover로 빛 차단**
- **1280 x 720 pixel**의 각각의 값들은 Control Board를 통해 PC로 전송되며 PC에서 난수 추출 및 후처리

- Experiment Result



- 상온에서 CMOS 이미지 센서의 출력값의 누적 평균을 통해 얻은 실험데이터는 이상적인 **포아송 분포에 근접**
- 원시난수 생성 레이트가 **초당 약 6.8Mbit**까지 검증

KIST Quantum RNG (2)

❒ Randomness 검증

- Hankel matrix와 HMAC를 사용하여 후처리한 후, NIST에서 제공하는 SP800-90B에 따라 검증

Hankel matrix

Statistical Test	P-Value	Proportion	Result
Frequency	0.689019	80/80	Pass
Block frequency	0.739918	80/80	Pass
Cumulative sums	0.834308	80/80	Pass
Runs	0.559523	80/80	Pass
Longest run	0.980883	80/80	Pass
Rank	0.911413	79/80	Pass
FET	0.637119	80/80	Pass
Non-overlapping template	0.991468	80/80	Pass
Overlapping template	0.242986	80/80	Pass
Universal	0.186566	80/80	Pass
Approximate entropy	0.509162	80/80	Pass
Serial	0.911413	80/80	Pass
Linear complexity	0.689019	80/80	Pass

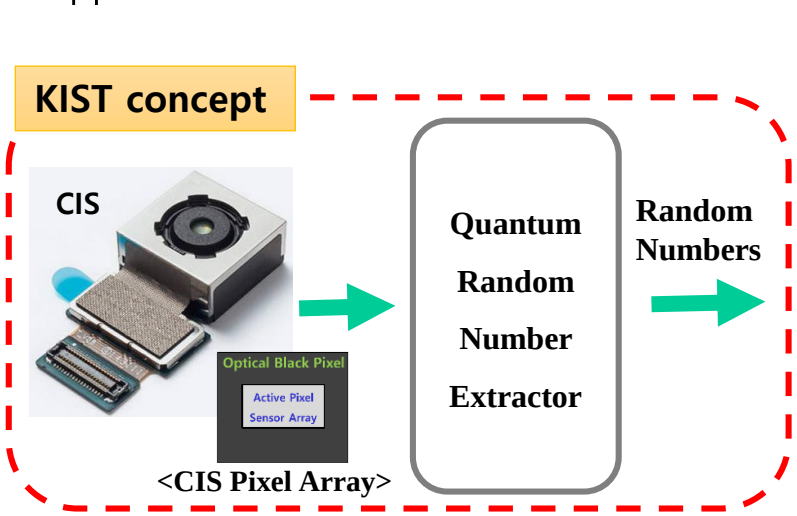
HMAC

Statistical Test	P-Value	Proportion	Result
Frequency	0.141256	80/80	Pass
Block frequency	0.811993	80/80	Pass
Cumulative sums	0.764655	80/80	Pass
Runs	0.371101	80/80	Pass
Longest run	0.227773	80/80	Pass
Rank	0.460664	80/80	Pass
FET	0.293235	80/80	Pass
Non-overlapping template	0.991468	80/80	Pass
Overlapping template	0.764655	79/80	Pass
Universal	0.980883	80/80	Pass
Approximate entropy	0.739918	80/80	Pass
Serial	0.311542	80/80	Pass
Linear complexity	0.611108	80/80	Pass

Hankel matrix, HMAC 후처리를 거친 난수의 엔트로피 측정 결과,
난수 test 항목 전부 통과

KIST Quantum RNG (3)

❒ Application



- 핸드폰, 게임기, 노트북, 디지털 카메라 **등 CMOS 이미지센서를 구비한 디바이스 및 이미지센서와 네트워크로 연결되는 모든 전자기기에 보안성 제공**
- 이미지센서를 활용하고 다른 하드웨어 없이 **소프트웨어적으로 양자난수발생**

❒ Patent

No.	출원번호 (출원일자)	발명의 명칭
1	제 10-2017-0119558 호 (17.09.18)	이미지센서를 이용한 난수 생성 시스템, 난수 생성 방법, 데이터베이스 구축방법, 및 그 방법이 컴퓨터 프로그램으로 기록되어 있는 컴퓨터 판독가능한 기록 매체

감사합니다