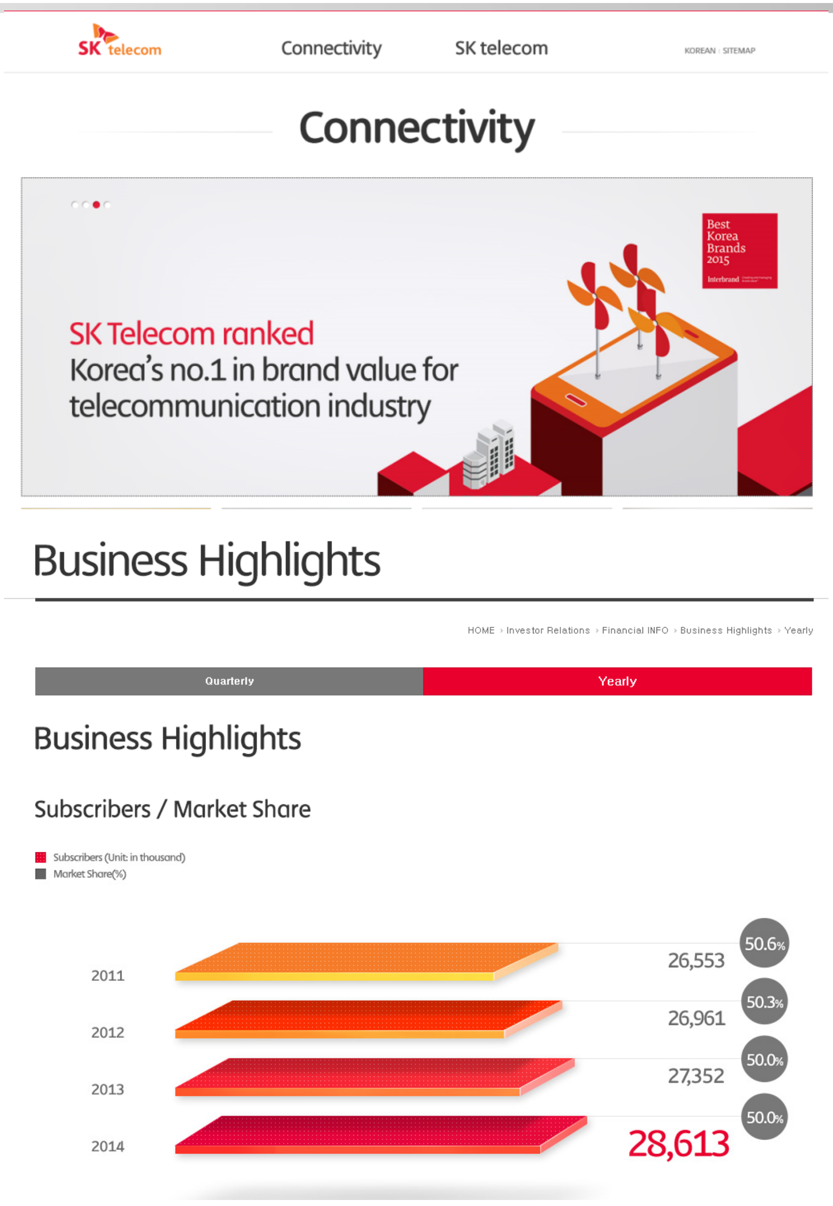
Introduction to SKT's QRNG
(A new approach for miniaturization of QRNG)

2016.05.03

Jeong Woon Choi
&
Sean Kwak

Quantum Tech. Lab
SK telecom

about SKT



Connectivity

SK Telecom ranked
Korea's no.1 in brand value for
telecommunication industry

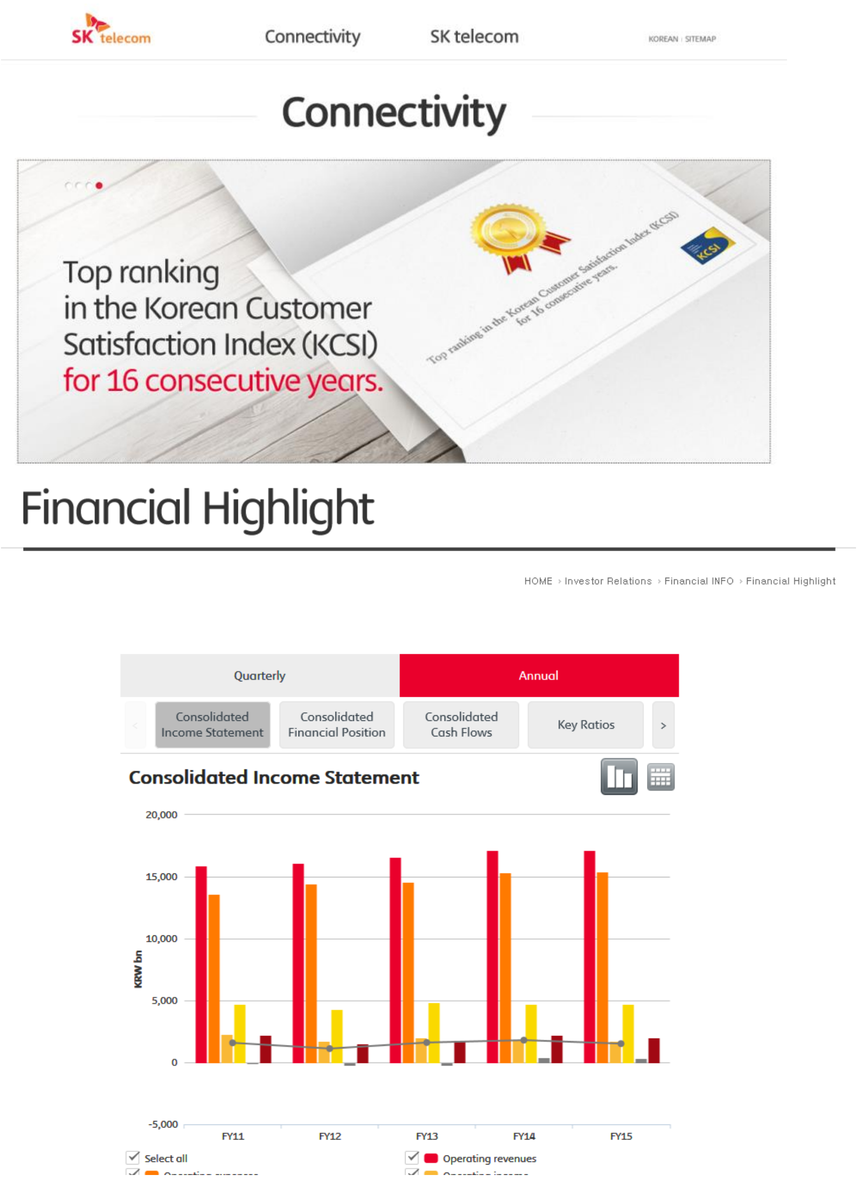
Business Highlights

HOME › Investor Relations › Financial INFO › Business Highlights › Yearly
Quarterly
Yearly

Business Highlights

Subscribers / Market Share

2011	26,553	50.6%
2012	26,961	50.3%
2013	27,352	50.0%
2014	28,613	50.0%



SK telecom
Connectivity
SK telecom
KOREAN · SITEMAP

Connectivity

Top ranking
in the Korean Customer
Satisfaction Index (KCSI)
for 16 consecutive years.

Top ranking in the Korean Customer Satisfaction Index (KCSI) for 16 consecutive years.
KCSI

Financial Highlight

HOME › Investor Relations › Financial INFO › Financial Highlight
Quarterly
Annual
Consolidated Income Statement
Consolidated Financial Position
Consolidated Cash Flows
Key Ratios
›

Consolidated Income Statement

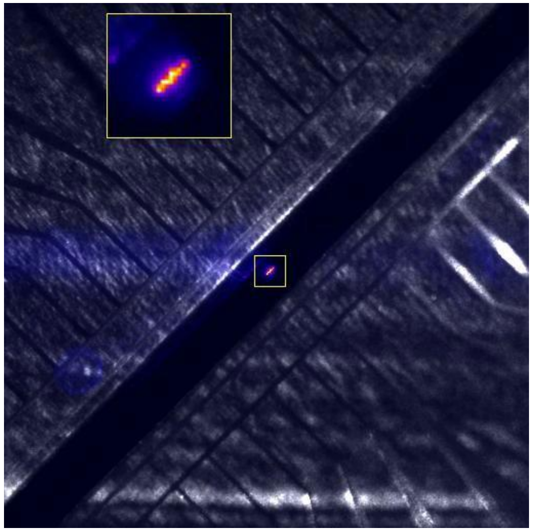
20,000
15,000
10,000
5,000
0
-5,000
KRW bn
FY11
FY12
FY13
FY14
FY15
☑ Select all
☑ 🟥 Operating revenues

about Quantum Tech. Lab in SKT (2011~)

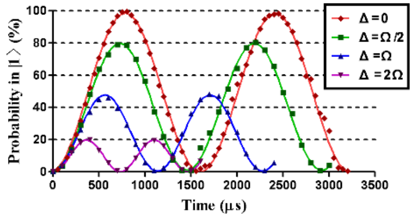
QKD

- 2014 World IT Show
- 2015 Mobile World Congress
- 2015 Congress Office at the Capitol Hill
- 2015 NGAUS general conference
- 2015 National Assembly of Korea

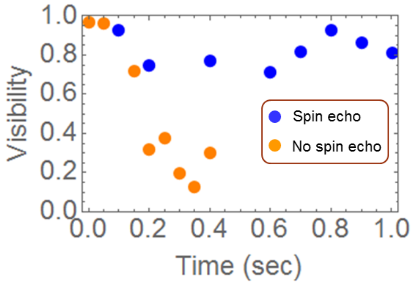
Ion-trap based Quantum Repeater



6 ions trapped by MEMS ion trap chip



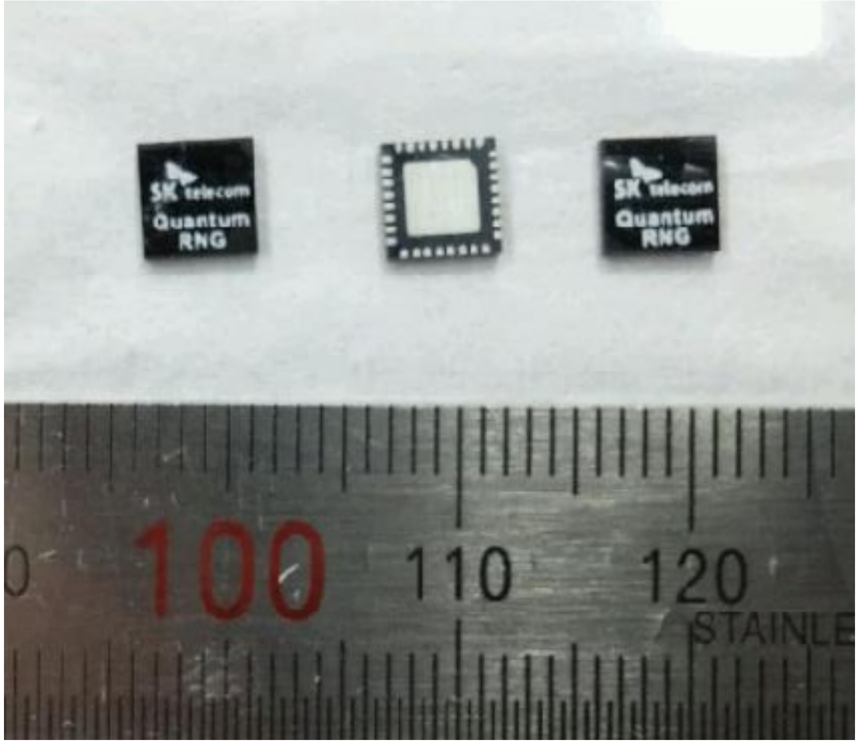
Rabi oscillation meas. w/ fitting



Ramsey fringe visibility w.r.t. time

- Design and fabrication of MEMS ion trap chip in Korea
- Trapping and shuttling of Yb ions
- Confirmed/extended coherence time by spin echo
- Working towards development of quantum repeater using ion traps

Today's Topic



QRNG

Quantum Random Number Generator (QRNG)

- **based on the non-deterministic properties of quantum physics (mostly, quantum optics)**
- **easy to understand the origin of randomness**
- **high-quality and high-speed**
- **but large and complicated a little bit**

[Quantis, IDQuantique]

- **4Mbps**
- **PCIe, USB**
- **photon dispersion**

[PQRNG150, PicoQuant]

- **150Mbps**
- **USB**
- **photon arrival time**

[qStream, Quintessence Lab]

- **1Gbps**
- **KMIP**
- **Fluctuation of vacuum states of light**

[Whitewood Entropy Engine, Whitewood Encryption Systems]

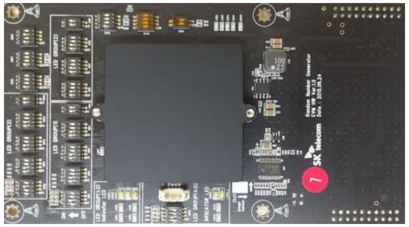
- **200Mbps**
- **PCIe**
- **bunching property of indistinguishable photons**

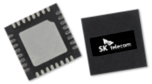
SKT's QRNG

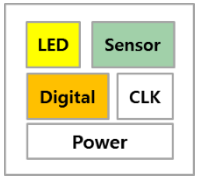
SKT QRNG module

[Previous/Current]
non-commercial

SKT QRNG chip






LED
Sensor
Digital
CLK
Power

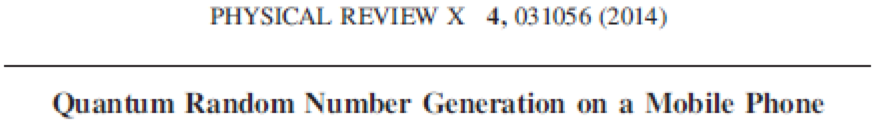
[Future]
commercialized

Performance	1Gbps x 2ch. (SHA-256 post-processing)
Size	140mm x 100mm x 20mm
Applications	QKD, various Servers and equipment
Physics	Quantum phase noise
IPR	University of Toronto

	Chip type	CAN type
Performance	Mbps	Gbps
Size	~ 5mm x 5mm	~ 50mm x 50mm
Applications	supporting all kinds of devices requiring RNG	
Physics	Quantum shot noise	
IPR	Exclusive License from IDQ, University of Geneva	

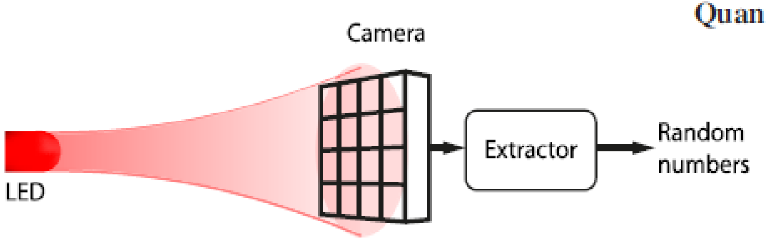
SKT's QRNG chip

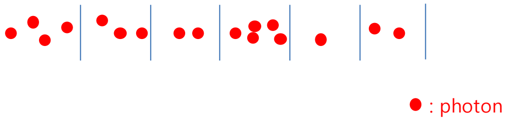
[Basic Principle of SKT QRNG]



PHYSICAL REVIEW X 4, 031056 (2014)

Quantum Random Number Generation on a Mobile Phone

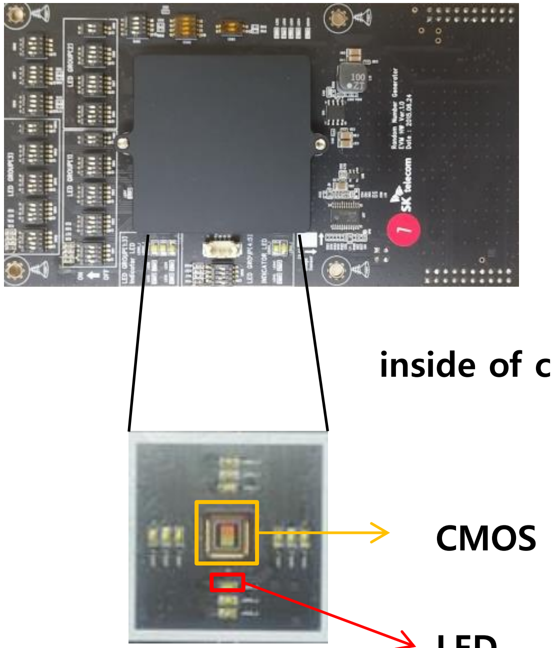




- LED (Light Emitting Diode) or other light source generates individual photons in a random or non-deter ministic time. More precisely, the number of detected photons in a certain fixed time interval varies ever y time due to quantum uncertainty.
- The number of photons detected in each pixel of CMOS sensor during any given exposure time follows the statistics of Poisson Distribution in which the mean (m) and variance (σ^2) have the same value in the ory.
  - ❖ The brighter the LED is, the more fluctuated the output of sensor has.
  - ❖ Of course, LED should be controlled in valid range in order to make quantum randomness dominant and prevent from saturation

SKT’s QRNG chip – evaluation (2015)

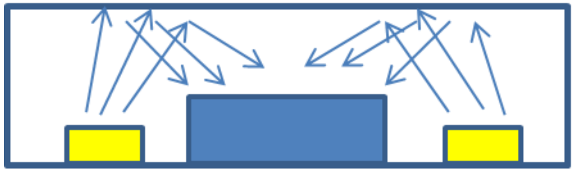
[Evaluation board + GUI]



inside of case

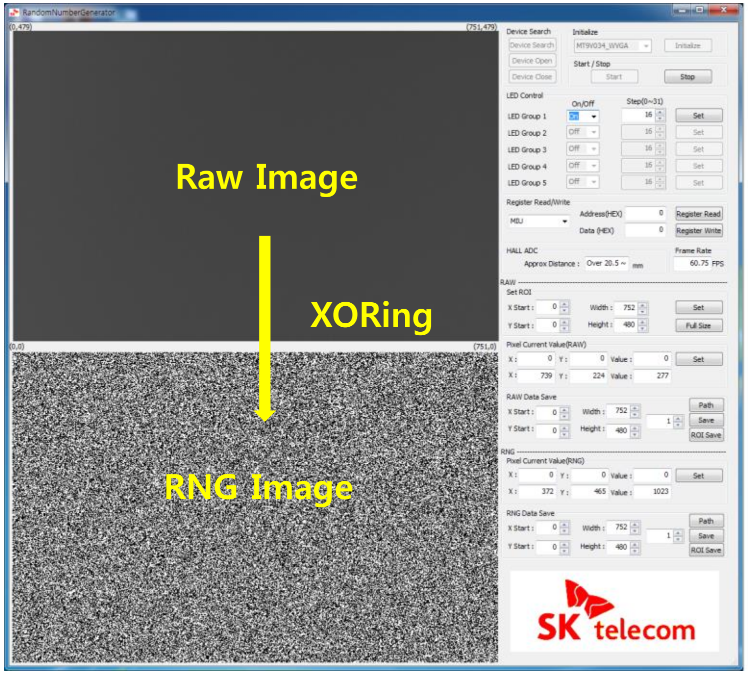
CMOS image sensor

LED



LED Sensor LED

LED → Sensor
: light is reflected and attenuated



Device Search
Initialize: MT9V034_WVGA
Start / Stop

LED Control

	On/Off	Step(0~31)
LED Group 1	On	16
LED Group 2	Off	16
LED Group 3	Off	16
LED Group 4	Off	16
LED Group 5	Off	16

Register Read/Write
MIU
Address(HEX) 0
Data (HEX) 0

HALL ADC
Approx Distance : Over 20.5 ~ mm
Frame Rate 60.75 FPS

RAW
Set ROI
X Start : 0 Width : 752
Y Start : 0 Height : 480

Pixel Current Value(RAW)
X : 0 Y : 0 Value : 0
X : 739 Y : 224 Value : 277

RAW Data Save
X Start : 0 Width : 752 1
Y Start : 0 Height : 480

RNG
Pixel Current Value(RNG)
X : 0 Y : 0 Value : 0
X : 372 Y : 465 Value : 1023

RNG Data Save
X Start : 0 Width : 752 1
Y Start : 0 Height : 480

[RNG image frame construction]

For each individual pixel of the raw image frame, we respectively extracted only one random bit, which is done by applying XOR operation to the LSB 3 bits of the10bit sensor pixel output.

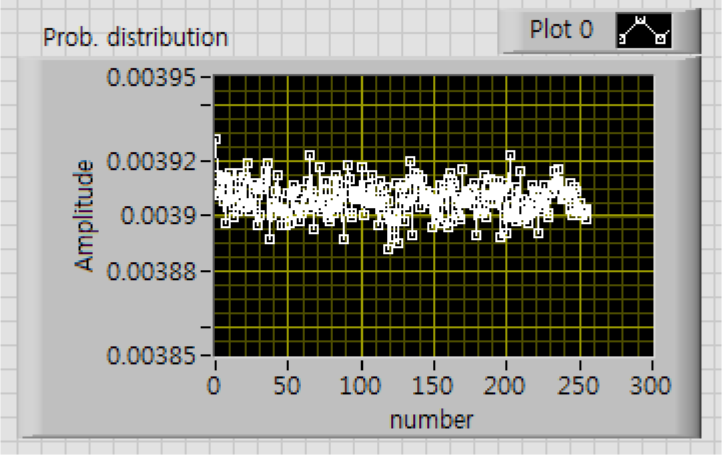
SKT's QRNG chip – evaluation result (2015)

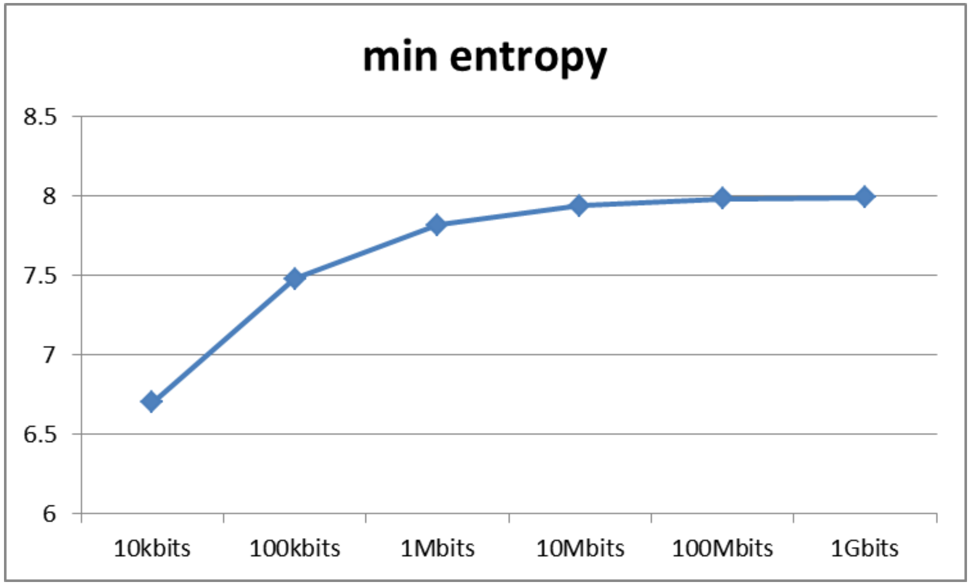
Min-entropy for RNG image data]

Min-entropy test for 1Gbit sample (test unit size = 1 byte)

[Result]

- max_prob. = 0.0039277
- ideal case: max_prob. = uniform prob. = 1/256 = 0.00390625
- **min-entropy = 7.9921**
- **It follows the law of large number, asymptotically close to the theoretical maximum as the size of sample gets larger**



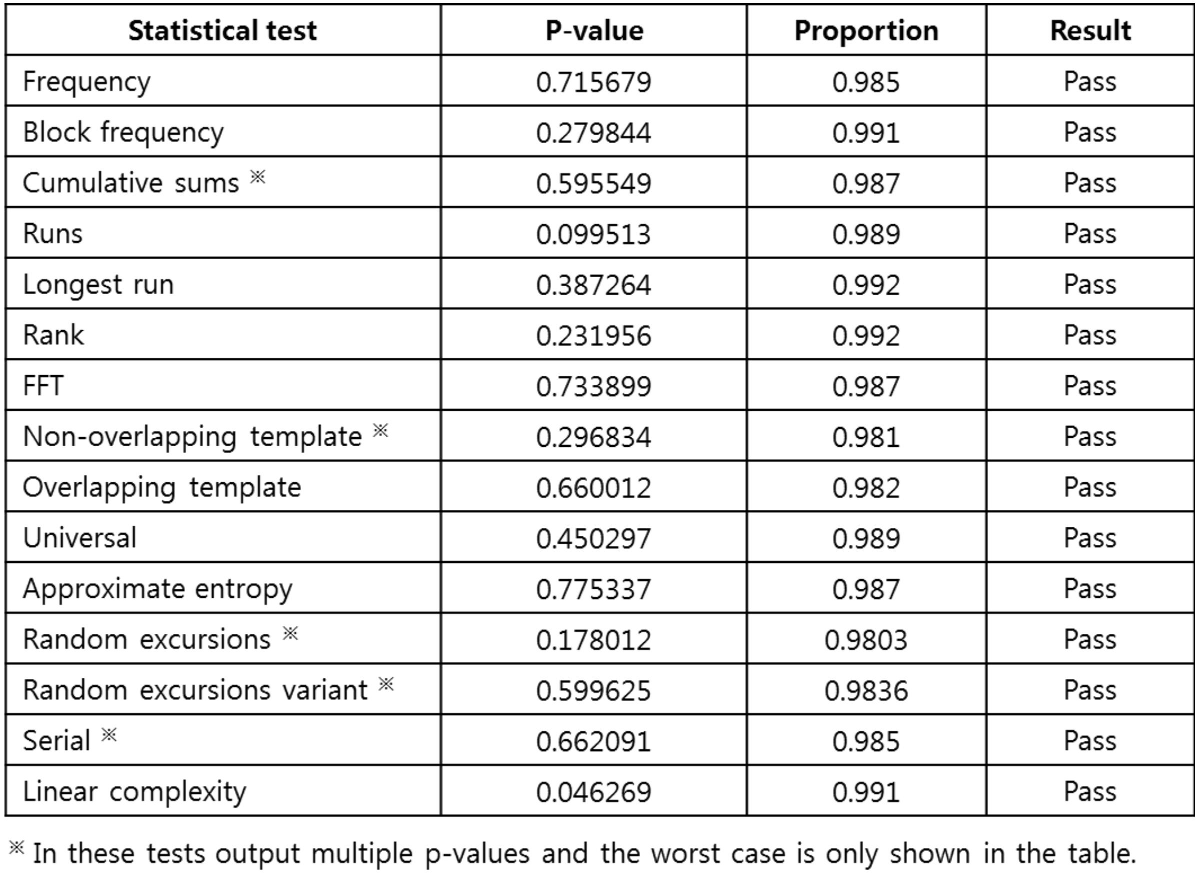


SKT’s QRNG chip – evaluation result (2015)

[SP 800-22 test for RNG image data]

SP 800-22 test with an RNG image sample of 1 Gbits
(sample size: 1 Mbit, # of queries: 1000)
[Result]

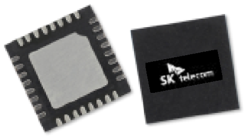
- normally pass all the test items
- but sometimes Block frequency or Non-overlapping fail



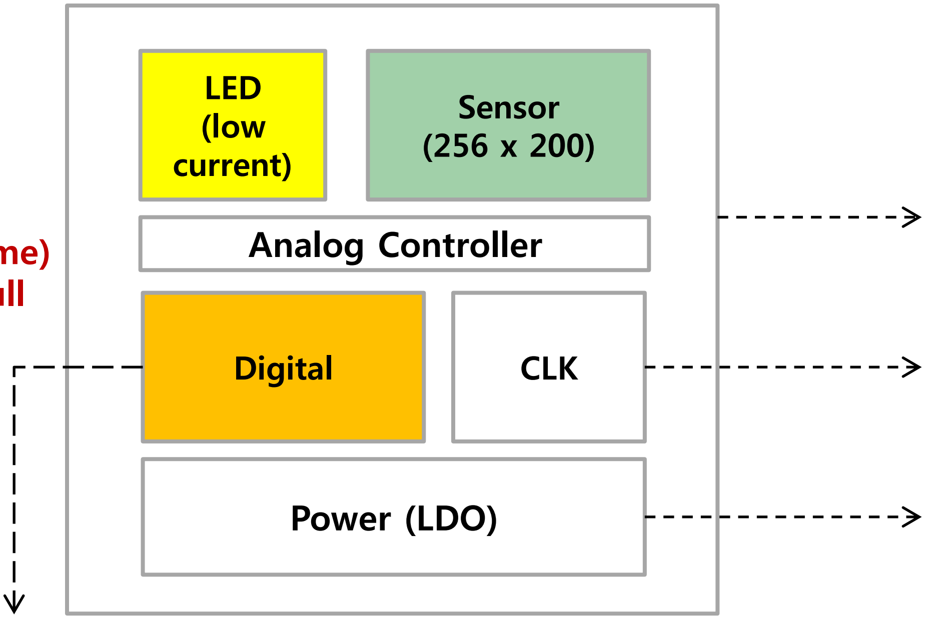
Statistical test	P-value	Proportion	Result
Frequency	0.715679	0.985	Pass
Block frequency	0.279844	0.991	Pass
Cumulative sums ※	0.595549	0.987	Pass
Runs	0.099513	0.989	Pass
Longest run	0.387264	0.992	Pass
Rank	0.231956	0.992	Pass
FFT	0.733899	0.987	Pass
Non-overlapping template ※	0.296834	0.981	Pass
Overlapping template	0.660012	0.982	Pass
Universal	0.450297	0.989	Pass
Approximate entropy	0.775337	0.987	Pass
Random excursions ※	0.178012	0.9803	Pass
Random excursions variant ※	0.599625	0.9836	Pass
Serial ※	0.662091	0.985	Pass
Linear complexity	0.046269	0.991	Pass

※ In these tests output multiple p-values and the worst case is only shown in the table.

SKT's QRNG chip – Specification (2016)



- The smallest in the world (< 5mm x 5mm x 1.5mm)
- Full entropy rate > 1.5Mbps (= 128 bit x 200 row x 60 frame)
- Can provide any length of full entropy and any security strength
- Secure against side-channel attack



ESD(Electrostatic Discharge) protection

ring OSC with OTP for adjusting

secure (turn-off) against low/high voltage

Compliance with NIST SP 800-90 A/B/C

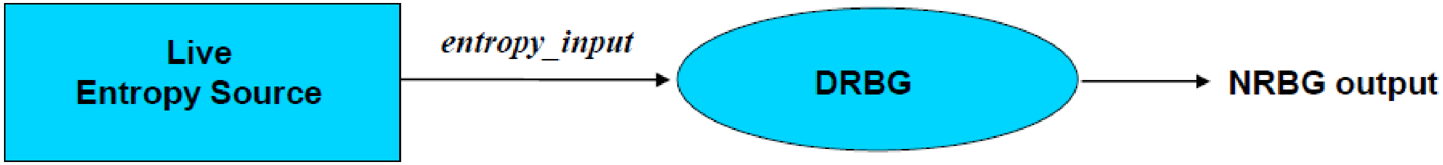
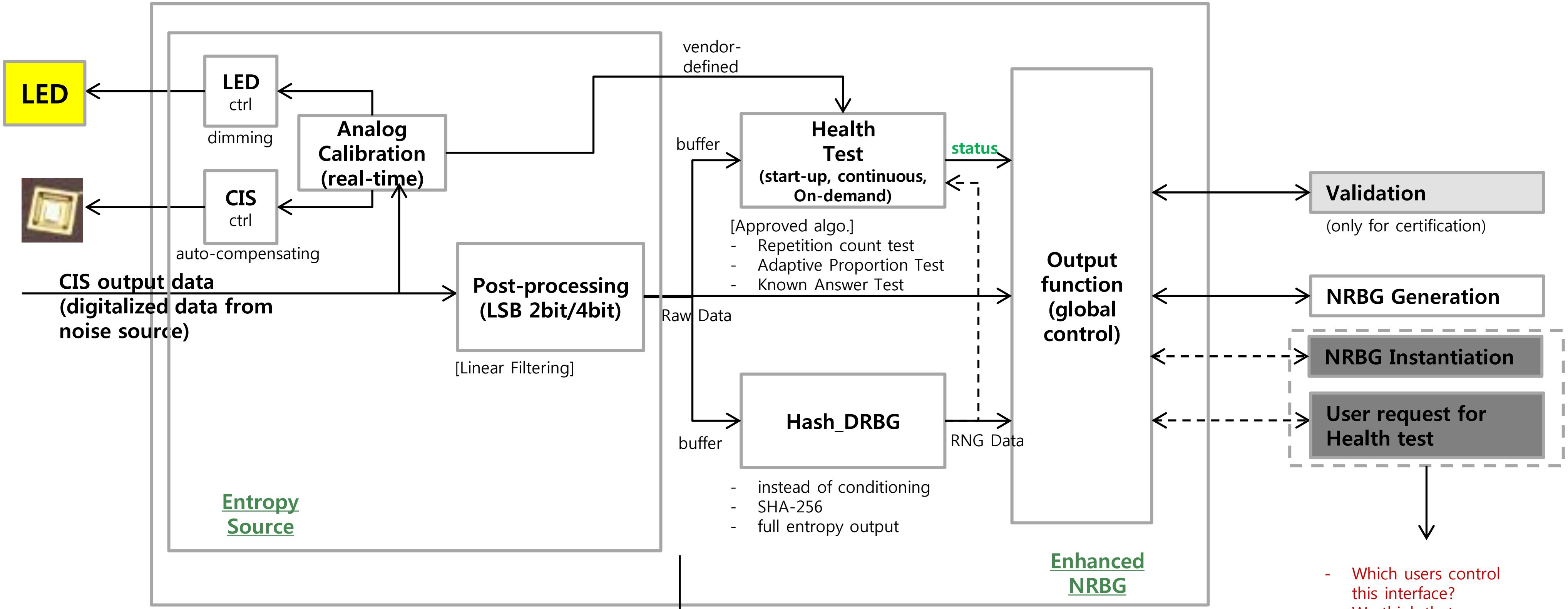


Figure 7: Enhanced NRBG - Oversampling Construction

SKT's QRNG chip – enhanced NRBG construction (SP 800-90B/C)



- Which users control this interface?
- We think that minimizing the commands from outside is more secure

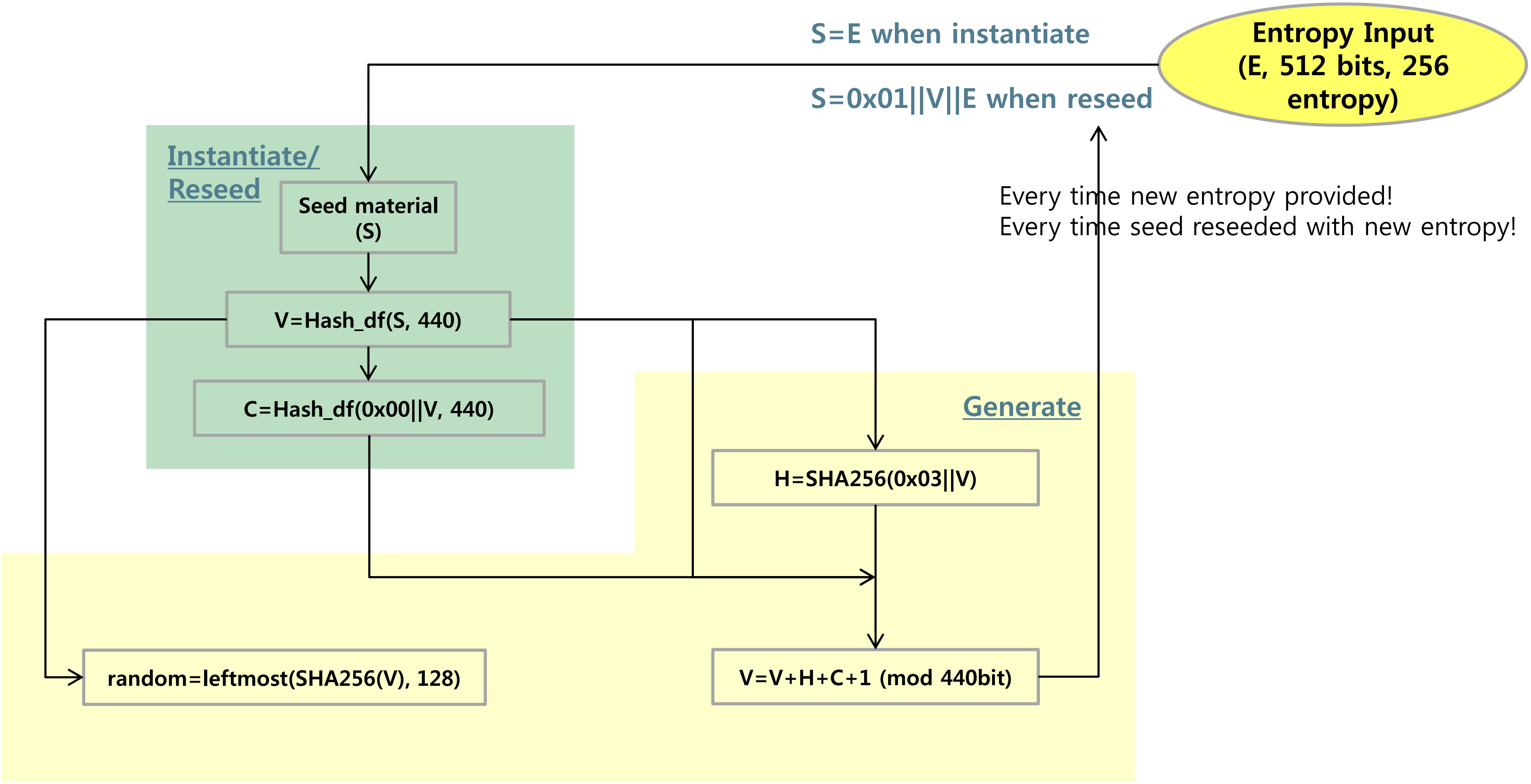
[Raw Data]

- 2-bit every clock
- 512-bit every row (256 pixel)
- at least 256 entropy every row

[RNG Data]

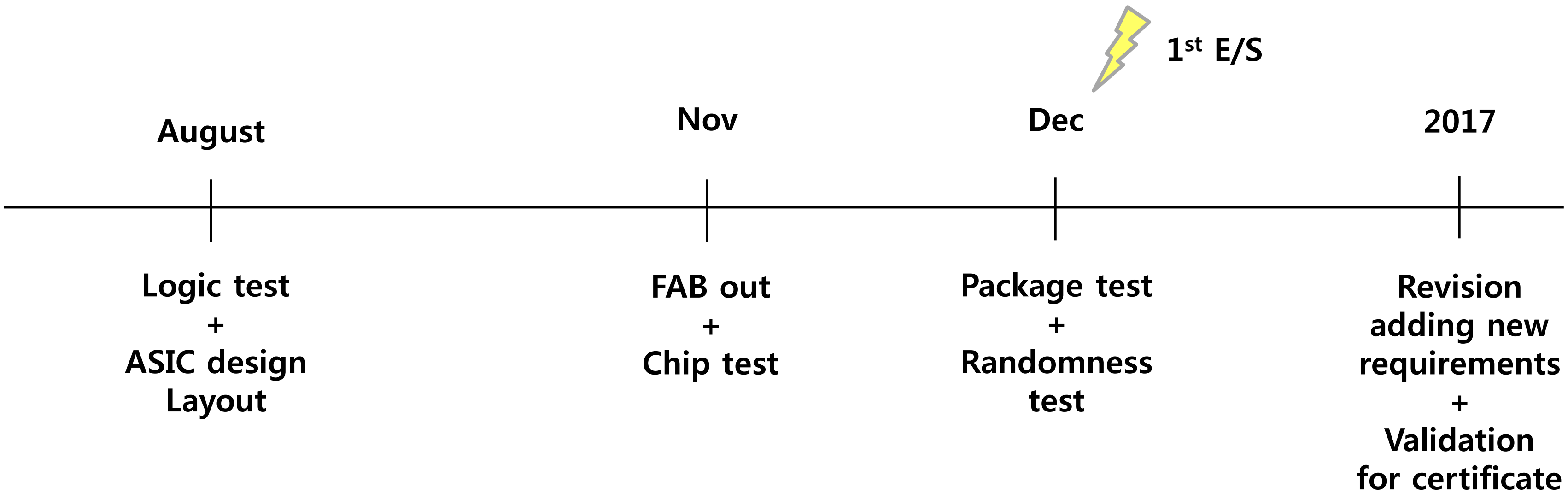
- 128-bit full entropy bit every row
- SHA-256 : 256-bit security strength
  → 128-bit full entropy for every input with 256 entropy (why half of security strength?)

SKT's QRNG chip - Hash_DRBG (NIST SP 800-90A)



※ Hash_df(x,440)=leftmost(SHA256(0x01||0x0…1B8||x)||SHA256(0x02||0x0…1B8||x),440)

SKT's QRNG chip - Development Plan for 2016



1st E/S

August

Logic test
+
ASIC design
Layout

Nov

FAB out
+
Chip test

Dec

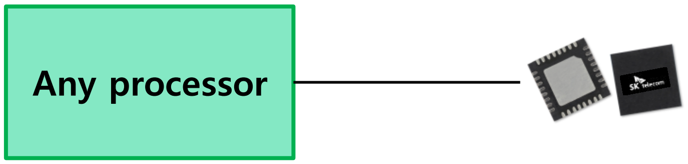
Package test
+
Randomness
test

2017

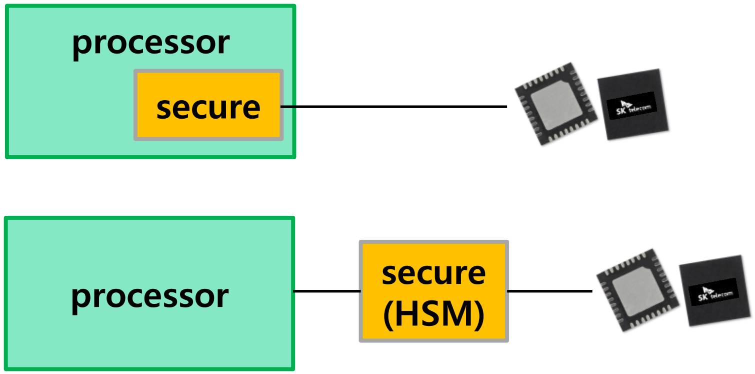
Revision
adding new
requirements
+
Validation
for certificate

SKT's QRNG chip - Applications

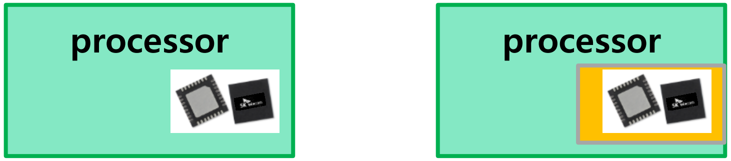
1) Stand-alone



2) Stand-alone but only accessible by secure area



3) Chip in Chip



4) Any combinations or multiple supports

IoT devices
Smart Car
PC
Server
Network equipment
Security Devices

Gambling
Simulation (Monte-Carlo)
Random processing (AI)

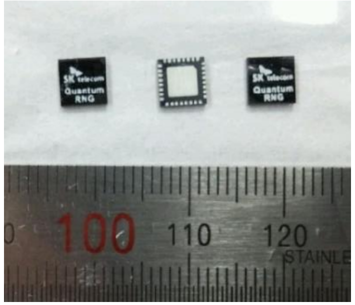
Summary – Our purpose

SKT's QRNG will provide

- the smallest and cheapest QRNG in the world
- high qualified and high rate randomness based on quantum shot noise
- reliability and consistency through transparent behavior
- easy to use, wide-spreading QRNG (beyond conventional Hardware-based RNGs)
- support environment without random source or with lack of entropy (IoT)
- enhance the security level of any devices

We welcome

- any comments
- any requirements
- any collaborations



[Contact Information]
jw_choi@sk.com
kwaksh@sk.com

Thank you !