Status of QKD system deployment and Ion Trap development at SK Telecom

Taehyun Kim

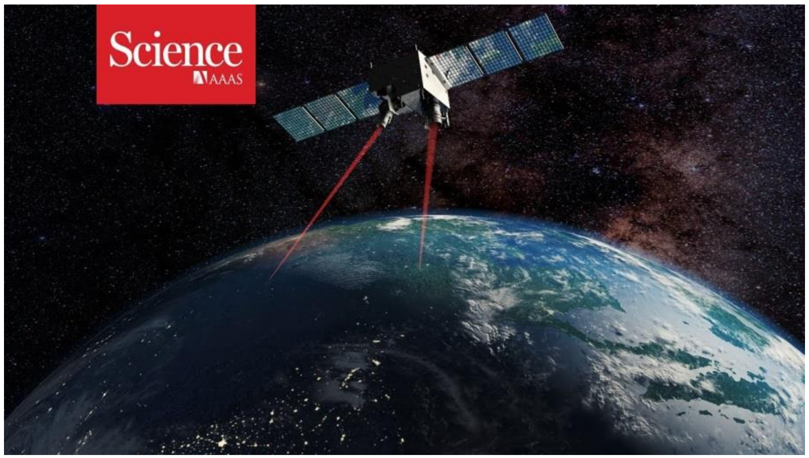
Quantum Tech. Lab, Corporate R&D Center

SK telecom

Quantum Satellite at China

Yin *et al.*, *Science* **356**, 1140–1144 (2017) 16 June 2017

Satellite-based entanglement distribution over 1200 kilometers



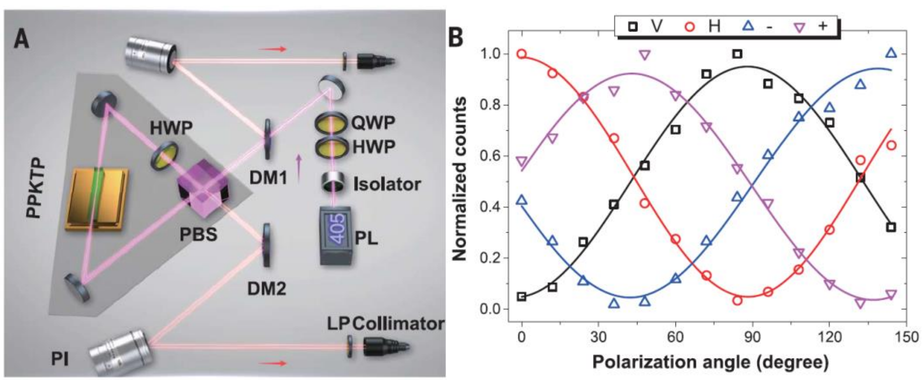
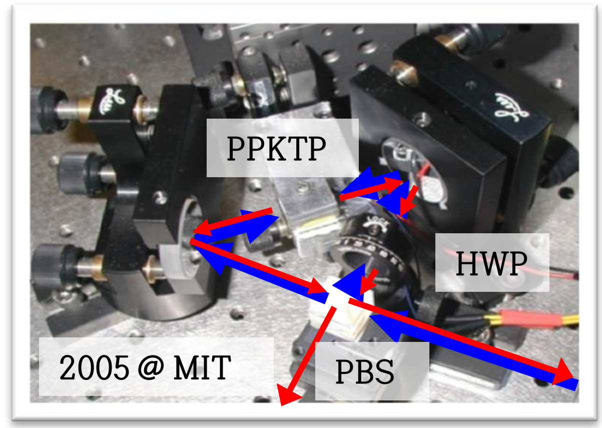


Fig. 1. Schematic of the spaceborne entangled-photon source and its in-orbit performance.

PHYSICAL REVIEW A **73**, 012316 (2006)

Phase-stable source of polarization-entangled photons using a polarization Sagnac interferometer

Taehyun Kim,* Marco Fiorentino,† and Franco N. C. Wong



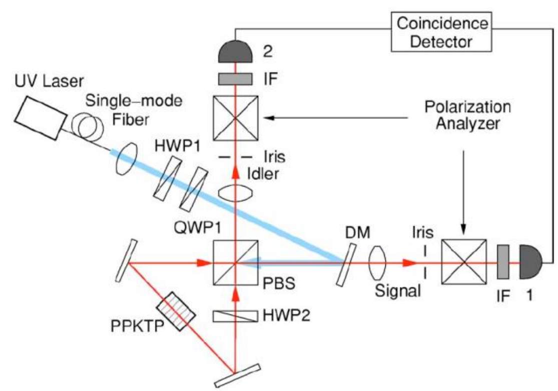
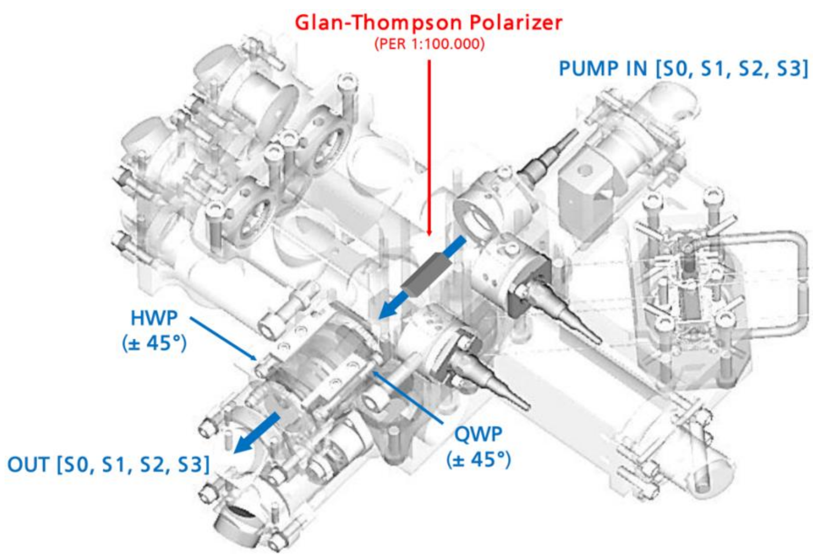
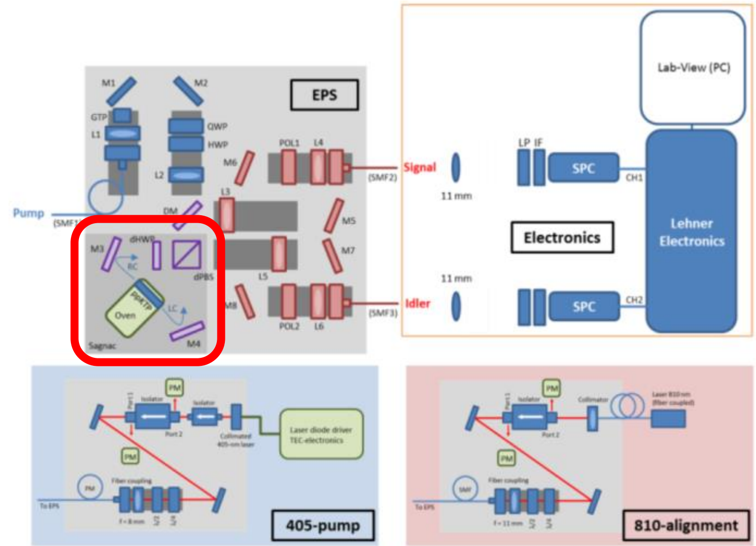


FIG. 2. (Color online) Experimental setup for polarization Sag-

Entanglement Source for European Quantum Satellite

- In an European conference for the quantum satellite supported by European Space Agency, entanglement source based on Sagnac interferometer is being considered as the entanglement source as well.
- “A space suitable engineering model of an entangled photon source (EPS)”





Polarization entanglement source based on Sagnac Scheme

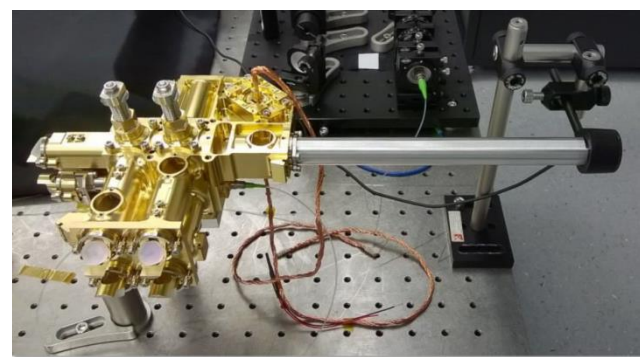


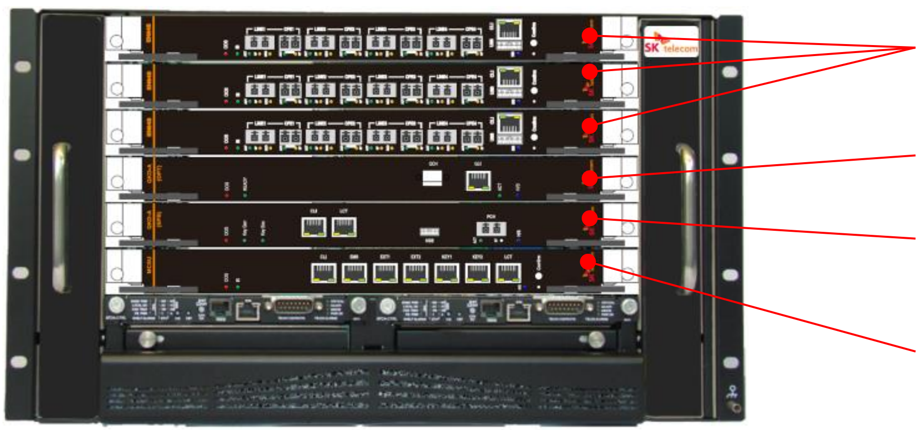
Table of Contents

- Overview of quantum key distribution (QKD) system development at SK telecom
- Overview of quantum random number generator (QRNG) development at SK telecom
- Development of quantum repeater at SK telecom
  - Ion trap chip development
  - Long coherence time measurement with sympathetic cooling

Quantum Key Distribution (QKD)

QKD at SK telecom

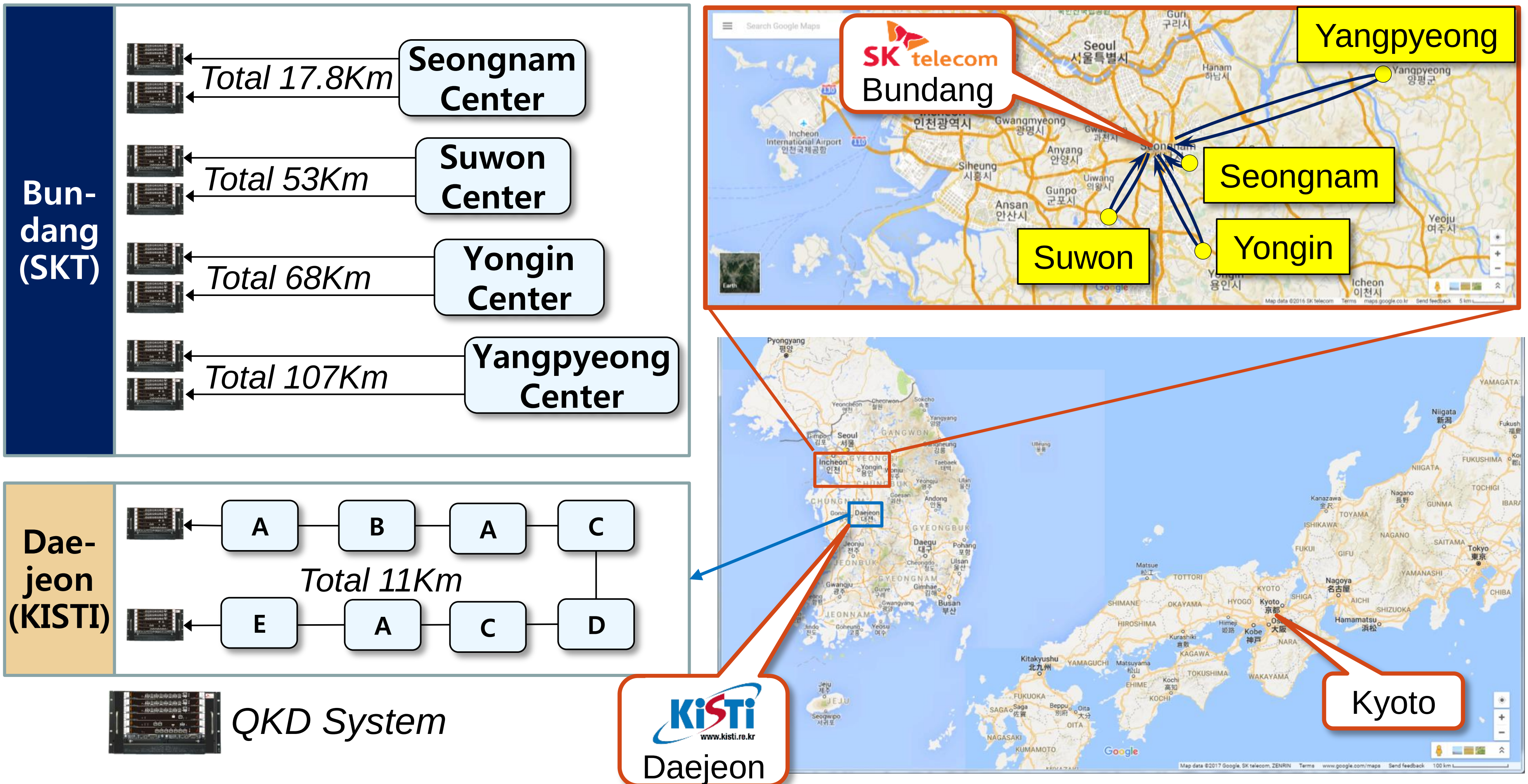
- **SKT QKD system is based on ATCA(Advanced Telecommunication and Computing Architecture) and easily extend the capacity of encrypted data by adding encryptor slots.**
- **Additionally, SKT is developing more flexible platforms like standalone QKD sever, etc.**



ATCA	
Chassis size	19 inch, 12U (14 slot) / 6U (6 slot); Shelf supplier dependent
QKD unit	2 slot
10Gbps encryptor unit	1 slot (bidirectional 4 ch.) ※ Max 80 slot (800Gbps)
Quantum key distribution	
Secure key rate	> 10 kbps @ 50km
Protocol	BB84 with unique phase modulation + decoy protocol and modified Winnow error correction
Random number generator	High speed quantum random number generator (2 Gbps)
Encryption	
Network protocols	10 GbE, STM64 (10 G SONET/OTN, 40G/100G Ethernet/OTN planned to be provided)
Algorithm	AES-GCM or ARIA-GCM
Latency	< 10 microseconds
Random number generator	Quantum random number generator

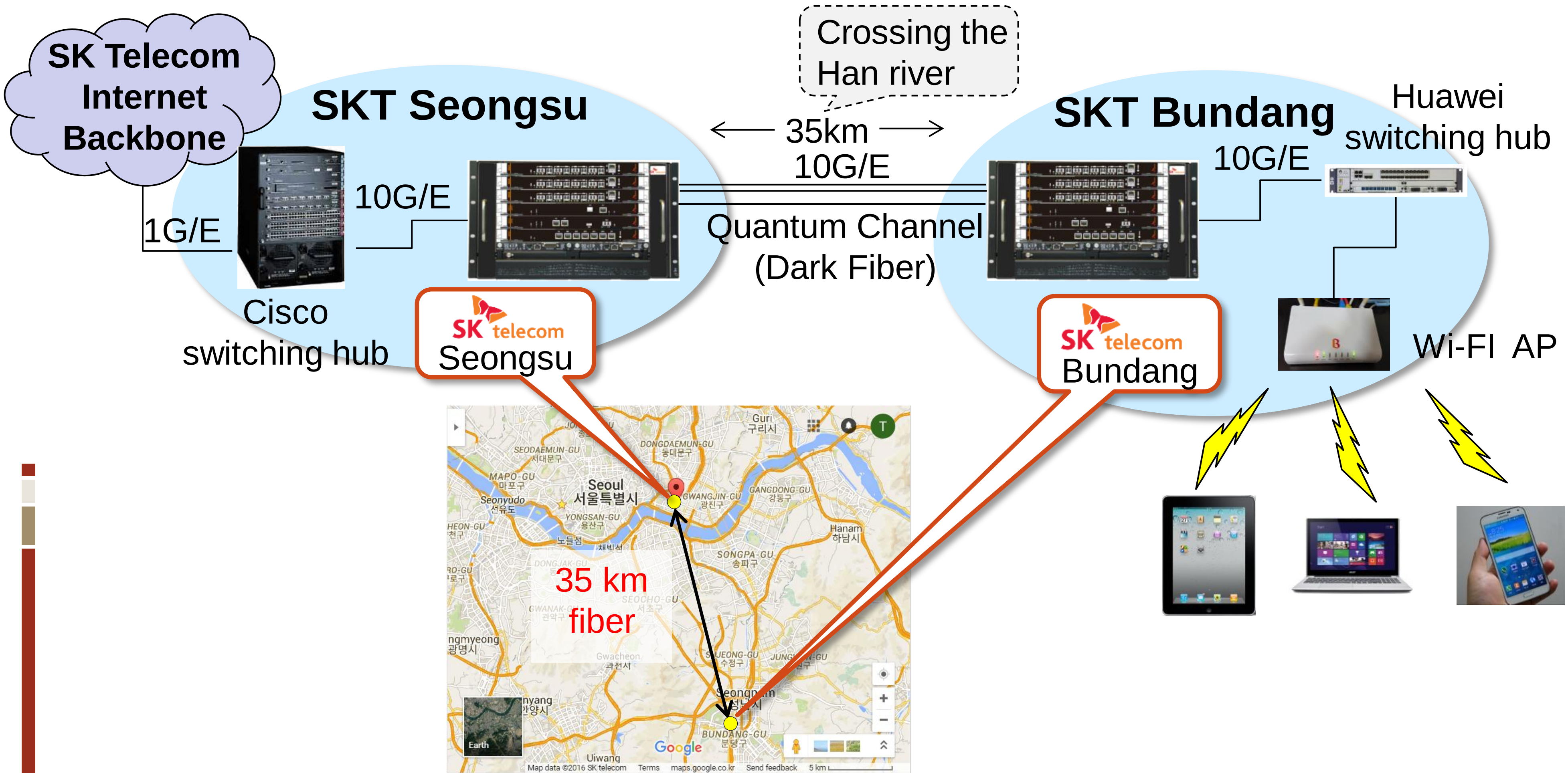
SKT & Korean Government QKD Test Bed

SKT and Korean government set up test beds for QKD systems around SKT R&D center located at Bundang area and also within national network R&D center located at Daejeon.



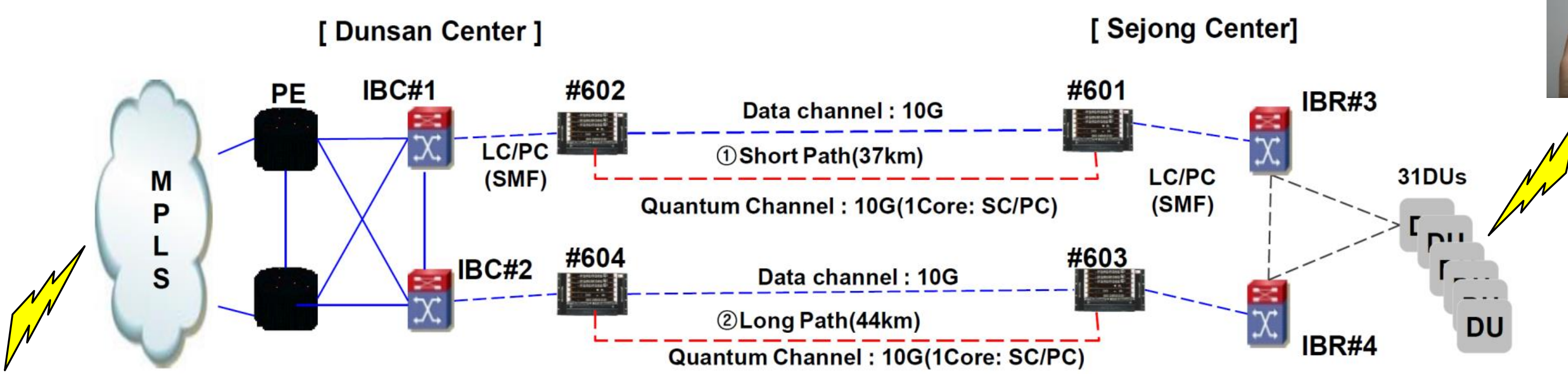
QKD connected to SKT Commercial Network

SKT deployed QKD system into its Wi-Fi commercial metro network in 2016.

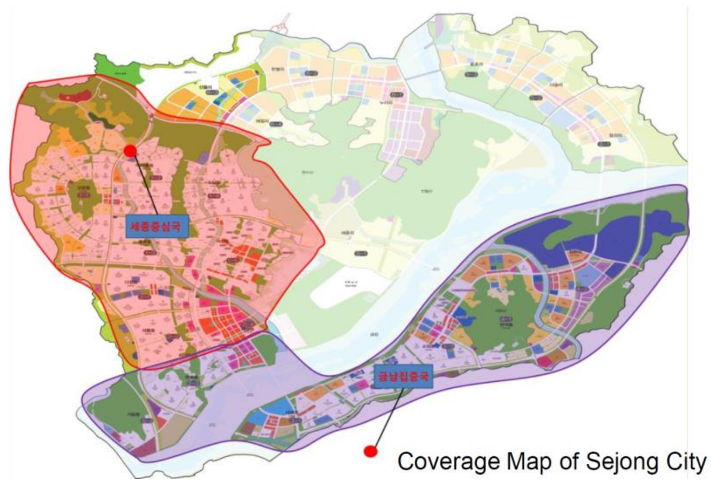


Incorporation of QKD system into 4G LTE network

- We also deployed a QKD system in 4G LTE commercial network in 2016



[Dunsan Center]



[Sejong Center]

Table of Contents

- Overview of quantum key distribution (QKD) system development at SK telecom
- Overview of quantum random number generator (QRNG) development at SK telecom
- Development of quantum repeater at SK telecom
  - Ion trap chip development
  - Long coherence time measurement with sympathetic cooling

Quantum Random Number Generator

- Background
  - Most of IoT devices use random number for security.
  - Most of current technologies rely on the pseudo random number generated by algorithm. However in many cases, it is possible to predict the probability distribution of pseudo random number generator.
  - Quantum random number generators (QRNG) are based on the non-deterministic properties of quantum physics. Therefore it is impossible to predict the probability distribution in principle.

[Quantis, IDQuantique]
- 4Mbps
- PCIe, USB
- photon dispersion

[PQRNG150, PicoQuant]
- 150Mbps
- USB
- photon arrival time

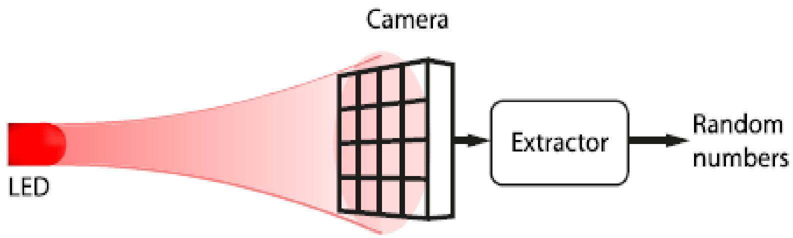
[qStream, Quintessence Lab]
- 1Gbps
- KMIP
- Fluctuation of vacuum states of light

[Whitewood Entropy Engine, Whitewood Encryption Systems]
- 200Mbps
- PCIe
- bunching property of indistinguishable photons

Development of QRNG chip

QRNG at SK telecom

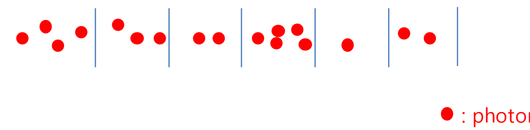
[Basic Principle of SKT QRNG]



PHYSICAL REVIEW X **4**, 031056 (2014)

Quantum Random Number Generation on a Mobile Phone

Bruno Sanguinetti,* Anthony Martin, Hugo Zbinden, and Nicolas Gisin
Group of Applied Physics, University of Geneva, Genève 4, CH-1211, Switzerland



- At SK telecom, we are developing QRNG chip composed of LED and CMOS sensor.
- The number of detected photons by each pixel follows the Poisson distribution even with thermal light from LED (Light Emitting Diode) when the detector is slow or the thermal light is multi-mode.
- Shot noise from Poisson distribution can be used as entropy source for random number generator.
- SK telecom has exclusive license from IDQ and University of Geneva

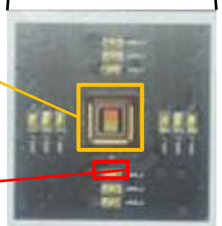
Test with prototype of QRNG chip

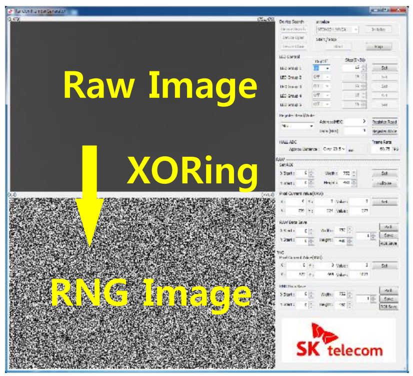
[Evaluation board + GUI]

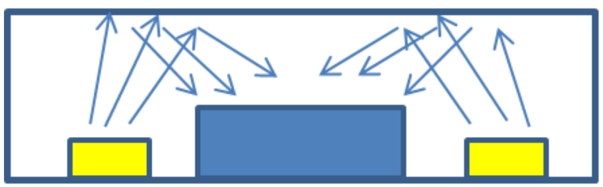
inside of case

CMOS image sensor

LED

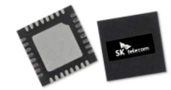


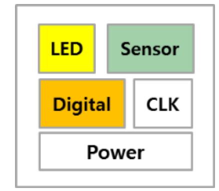




LED → Sensor
: light is reflected and attenuated

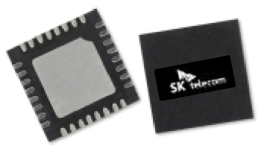
[Future]
commercialized



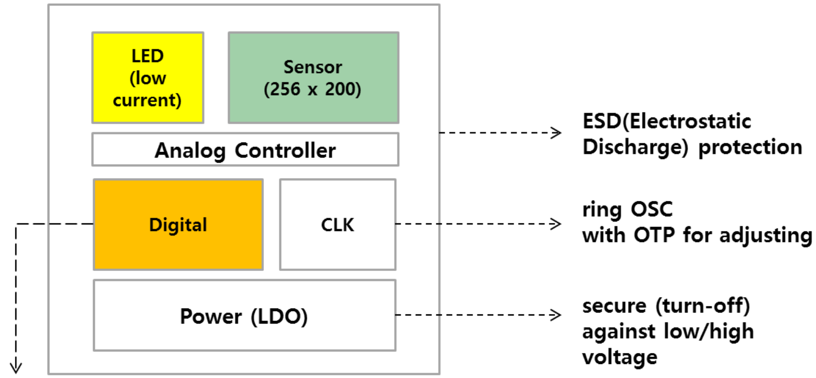


	Chip type	CAN type
Performance	Mbps	Gbps
Size	~ 5mm x 5mm	~ 50mm x 50mm
Applications	supporting all kinds of devices requiring RNG	
Physics	Quantum shot noise	

Progress of QRNG chip development



- Small form-factor (< 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



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

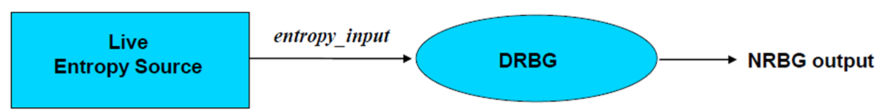


Figure 7: Enhanced NRBG - Oversampling Construction

1st E/S

Aug. 2016 — Logic test + ASIC design Layout

Nov. 2016 — FAB out + Chip test

Mar. 2017 — Package test + Randomness test

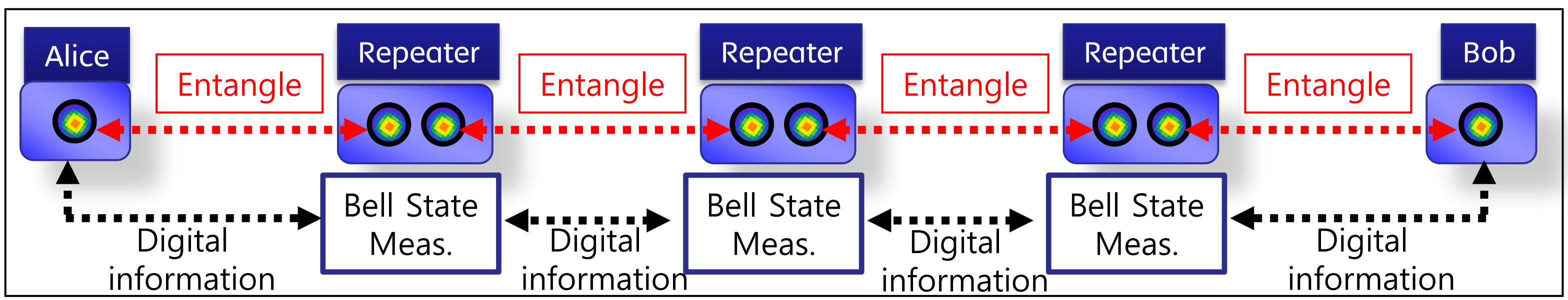
Dec. 2017 — Revision adding new requirements + Validation for certificate

Table of Contents

- Overview of quantum key distribution (QKD) system development at SK telecom
- Overview of quantum random number generator (QRNG) development at SK telecom
- Development of quantum repeater at SK telecom
  - Ion trap chip development
  - Long coherence time measurement with sympathetic cooling

Quantum Repeater

- At SK telecom, quantum repeater based on ion trap is required to expand the system over long distance
- Basic ingredients of quantum repeater
  - Generation of entangled states
  - Measurement of Bell states
  - Single qubit operation on the teleported qubits



Quantum Repeater based on Ion Trap

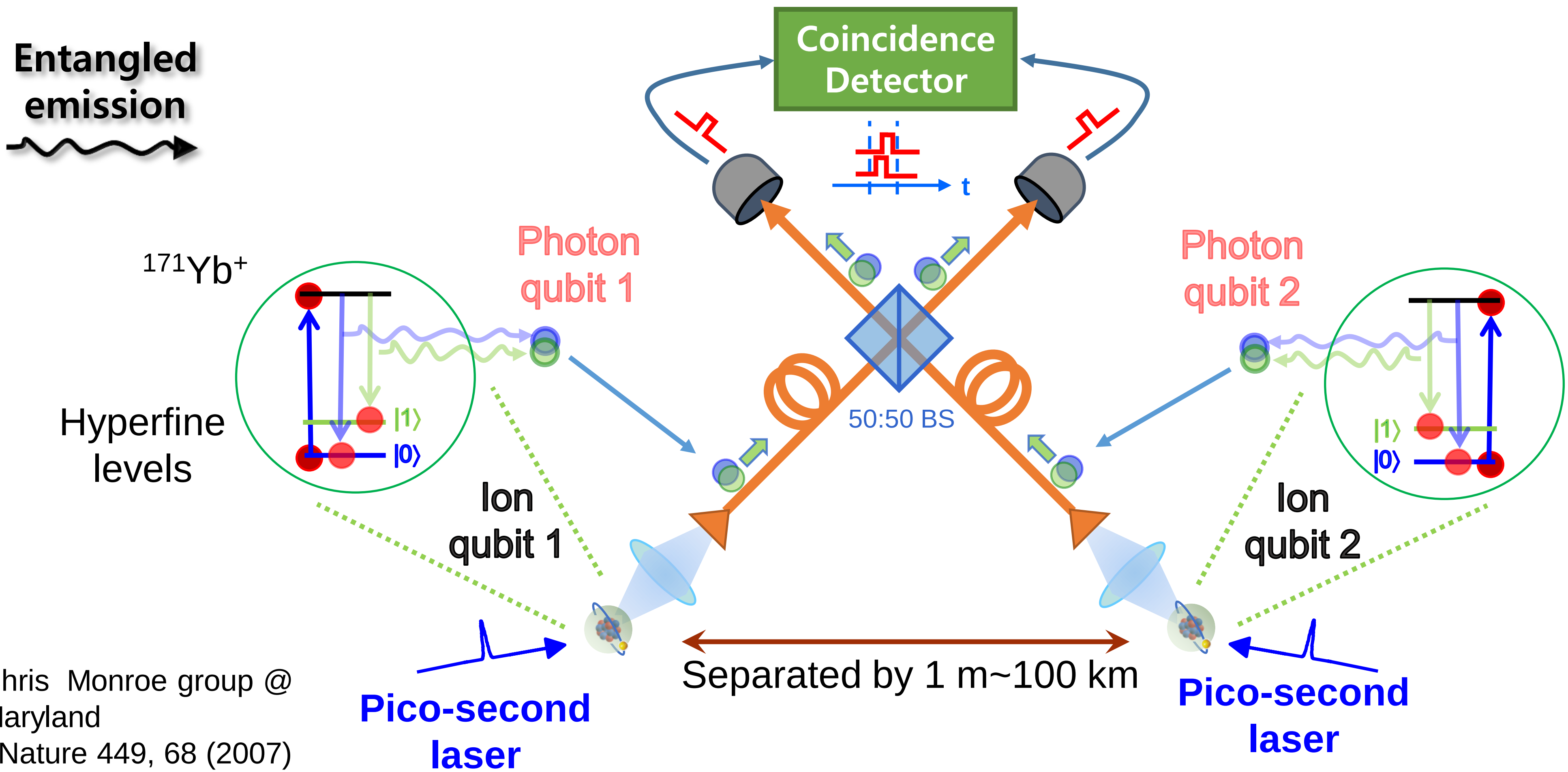
- **Advantage of trapped ions** as a platform for quantum repeater
  - Long coherence time: isolated from environment in ultra high vacuum (UHV) system
  - Long trapping time: charged particles are confined by electric field only
  - Deterministic two-qubit gate
  - Near-unity measurement efficiency with low error probability
  - Heralded generation of entangled states stored in stationary qubits
  - Scalability: many qubits can be trapped simultaneously
  - Each ions can be controlled individually: addressability with focused laser
- **Challenges** in the implementation of quantum repeater based on ion trap
  - Generation rate of heralded entangled state
  - Scalability
  - Deterministic, high-fidelity single-qubit and two-qubit gate operation
  - Entanglement over long distance

Table of Contents

- Overview of quantum key distribution (QKD) system development at SK telecom
- Overview of quantum random number generator (QRNG) development at SK telecom
- Development of quantum repeater at SK telecom
  - Ion trap chip development
  - Long coherence time measurement with sympathetic cooling

Generation of Entanglement

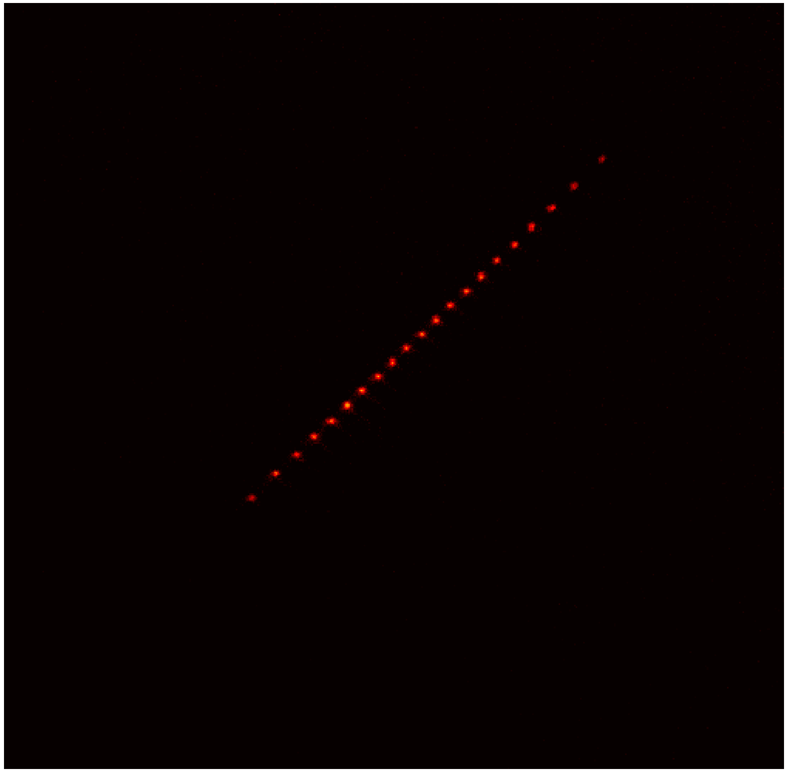
- Heralded entanglement generation between two ions separated by macroscopic distance



Chris Monroe group @ Maryland
- Nature 449, 68 (2007)

Trapping of ions and basic operations

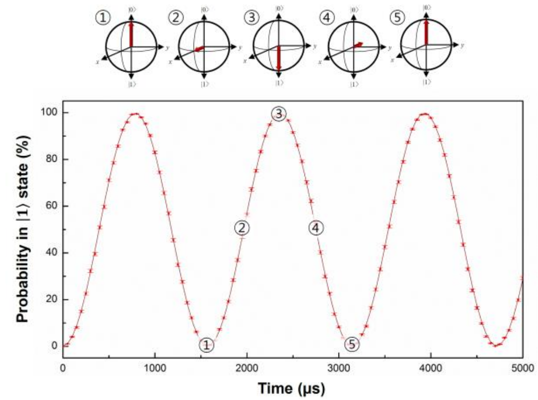
Experiment at SKT



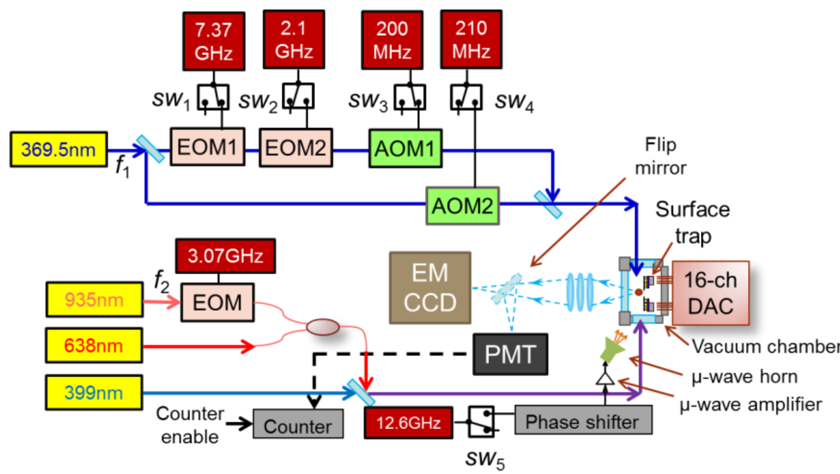
Step	Duration	sw$_1$	sw$_2$	sw$_3$	sw$_4$	sw$_5$	Counter enable
1. Doppler cooling	T_{cool}	on	off	on	off	off	off
2. Initialization	T_{init}	off	on	on	off	off	off
3. Rotation in Bloch sphere	T_{rot}	off	off	off	off	on	off
4. State detection	T_{detect}	off	off	off	on	off	on

Experimental procedure for Rabi oscillation measurement

- Rabi oscillation



Experimental result of Rabi oscillation measurement



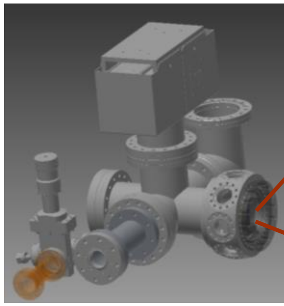
Experimental Setup for Rabi oscillation Measurement

Overview of Ion Trap Systems at SK telecom

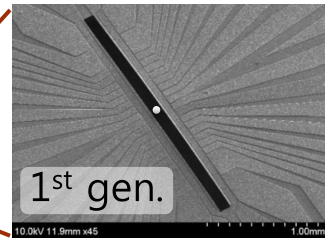
Experiments at SKT

- Development of 1st System

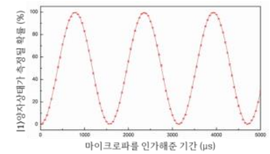
~600 mm



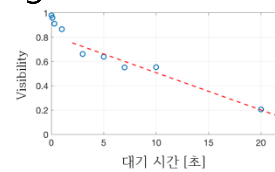
~3 mm



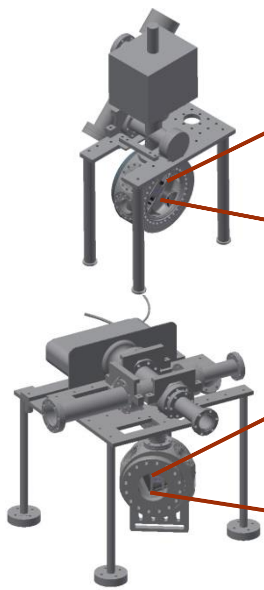
Rabi oscillation



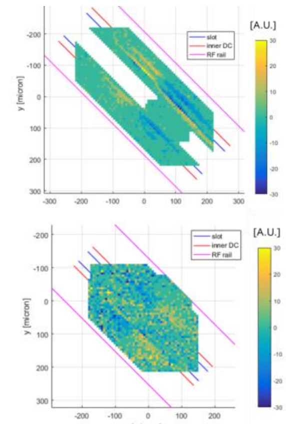
Long coherence time



- Development of 2nd System



Charging experiment



Entanglement Generation

2-qubit Gate

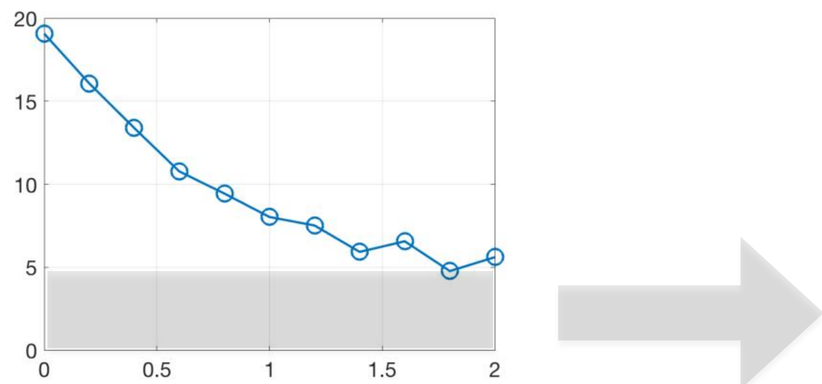
Table of Contents

- Overview of quantum key distribution (QKD) system development at SK telecom
- Overview of quantum random number generator (QRNG) development at SK telecom
- Development of quantum repeater at SK telecom
  - Ion trap chip development
  - Long coherence time measurement with sympathetic cooling

Sympathetic Cooling

- Motivation
  - Trapped ions are subject to motional heating, which prevents the proper evaluation of long coherence time of $^{171}Yb^{+}$ qubit
  - A heated ion escapes from the trap when it gains enough kinetic energy.
  - A heated ion scatters less photons during the state measurement, due to Doppler shift.

Average # of photons detected from $|1\rangle$ state over 100 μs

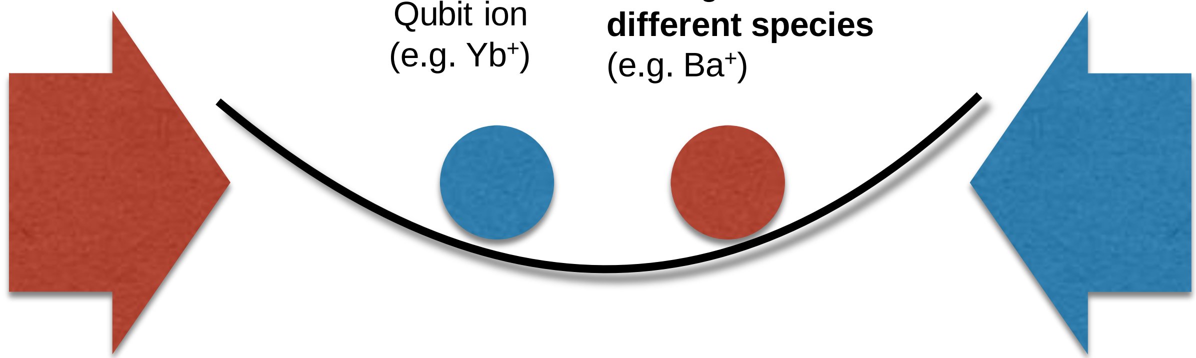


wait time before measurement [seconds]

classified as $|0\rangle$ state

Popular Approach for Sympathetic Cooling

Common implementation:



From Tsinghua University group, "Single-qubit quantum memory exceeding 10-minute coherence time," arXiv:1701.04195 (2017)

Increased cost and complexity of optical setup

Each species of trapped ion generally requires:

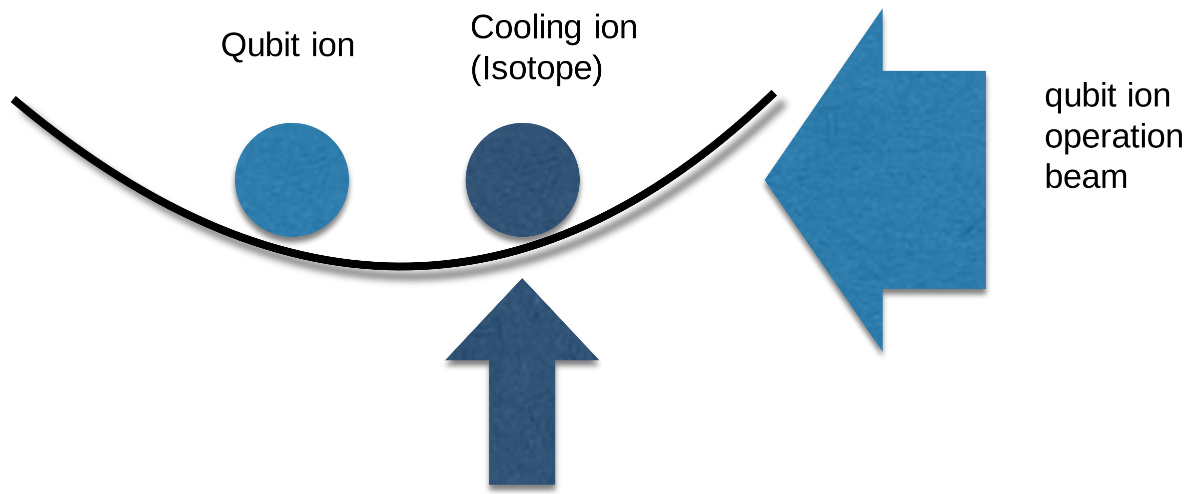
- Ionization beam
- Cooling beam
- Repumping beam (one or more)

Two sets of optical devices and components (filters, waveplates, lenses, EMCCD cameras, etc.)

Need more space and extra optical access

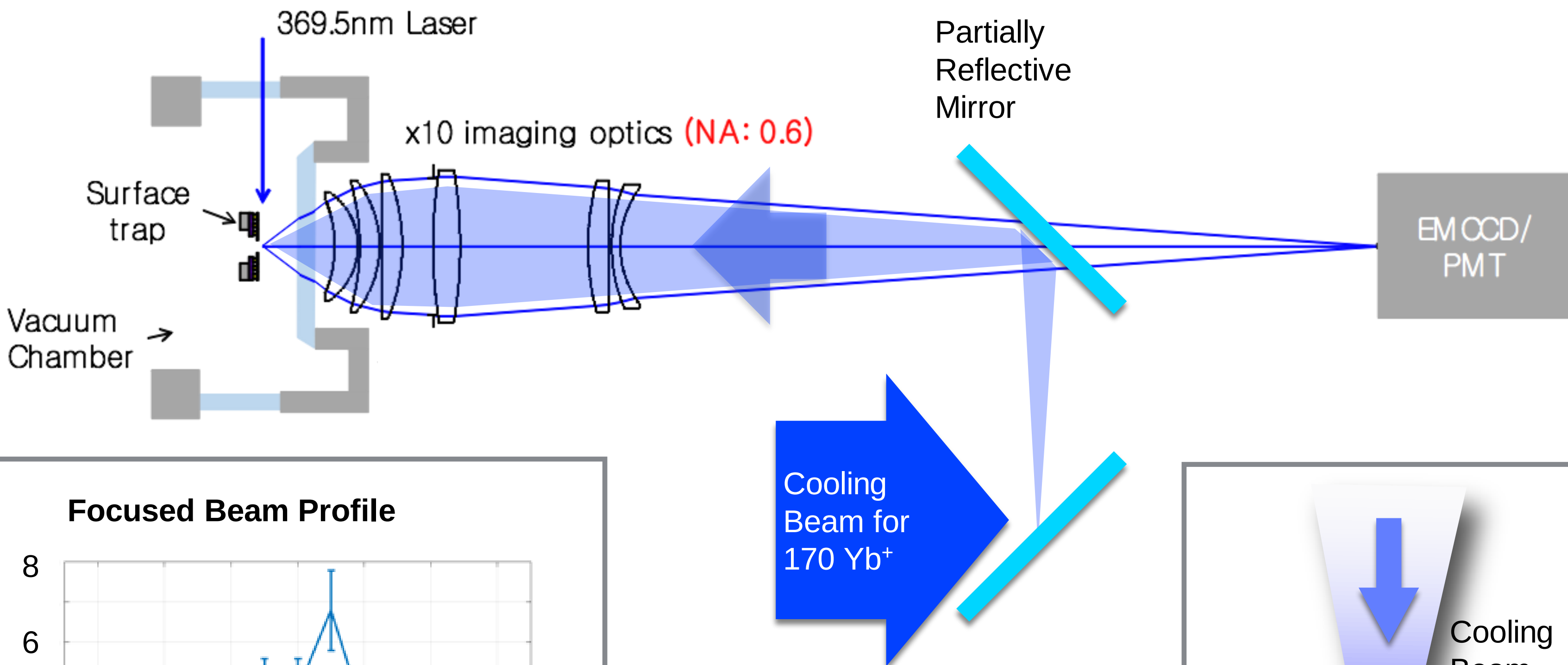
Different Approach for Sympathetic Cooling

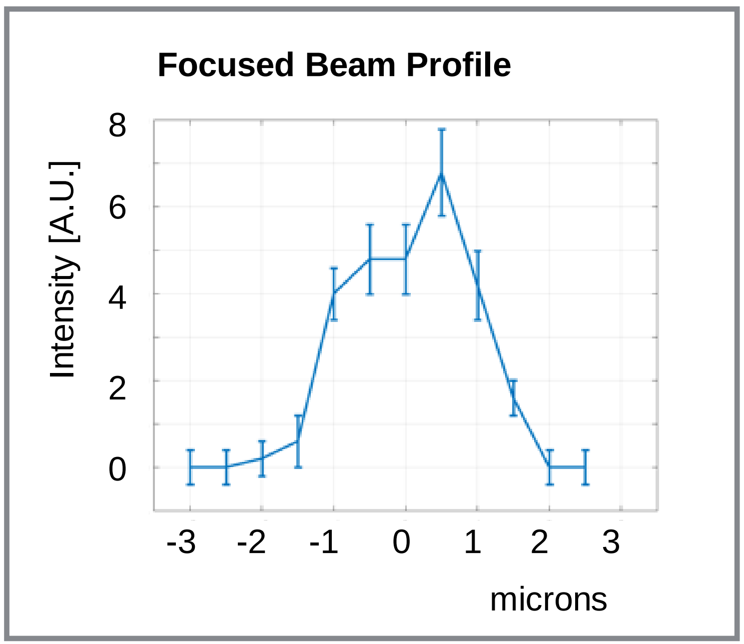
- Sympathetic cooling with a different isotope cooled by a focused laser



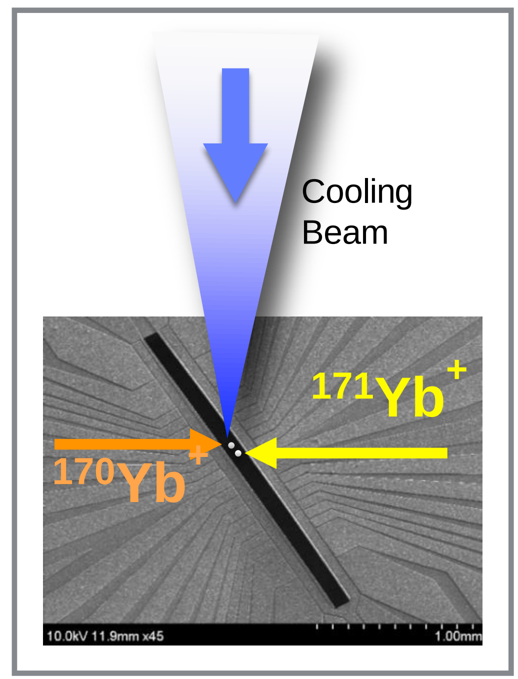
- Isotopes have similar energy level structures.
- Beams for each type of ion can be generated from a single source, frequency-adjusted by AOM or EOM.
- No need for two separate sets of optical devices and components.

Minimizing Exposure using Focused Cooling Beam





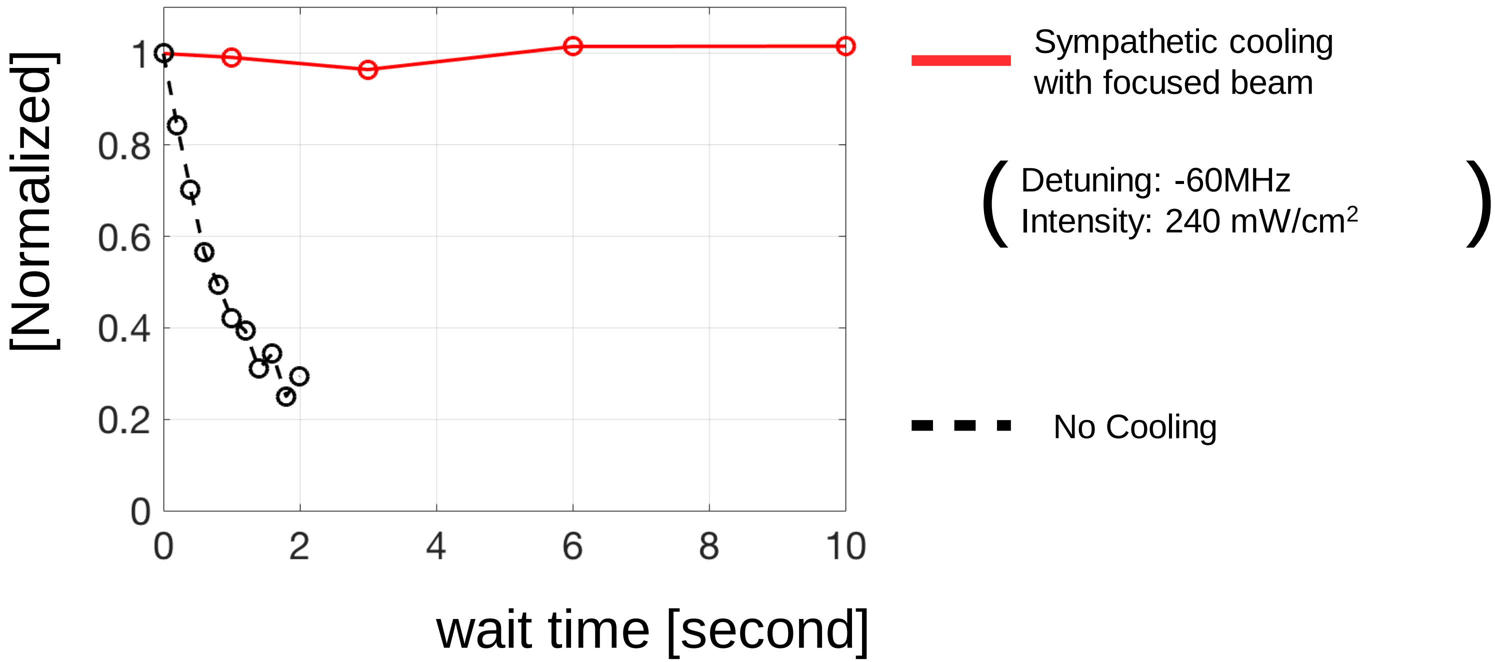
Ion-ion distance:
~ 5 microns



Sympathetic Cooling Result: Scattering Rate

Experiment at SKT

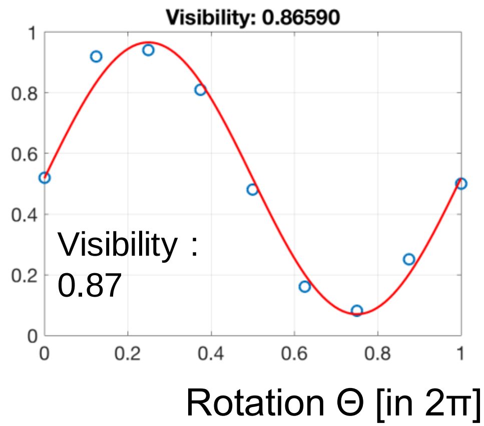
Scattering Rate



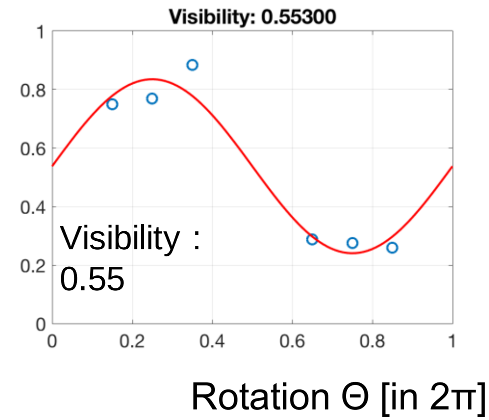
Coherence Measurement w/ Dynamic Decoupling

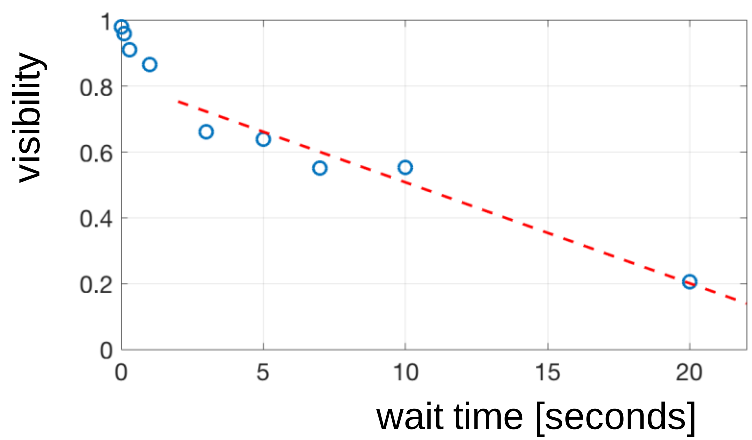
Experiment at SKT

1 second



10 second





Coherence time > 10 seconds

Summary

- QKD system is being installed in the commercial network in South Korea
- Chip-sized quantum random number generator is being developed and engineering sample is available now
- Development of a quantum repeater based on ion trap technology
  - Developed our own chip fabrication capability
  - Demonstrated basic ion trap capability such as trapping, shuttling, qubit state detection, and single qubit control
  - Observed coherence time about 10 seconds through sympathetic cooling with isotopic ion and dynamic de-coupling sequence
  - Developing systems to generate entanglement between two remote trapped ions
  - Working to implement two-qubit gate between two ions trapped in the same trap

Thank you