Summary

of

- The most advanced results of quantum cryptography, communications, metrology, and information processing were presented by 36 talks, 75 posters and 11 exhibitions.

- The number of registrations was totally 324, including 249 from scientific societies and 75 from government offices, enterprises and the press.

- Serious and fair discussions on the viability of quantum cryptography were made by modern and quantum cryptographers, and communication engineers. Vital challenges of quantum cryptography were addressed.

- In this document, current status and future challenges of quantum information and communications are summarized based on the presentations and discussions at the conference.

Quick look at talks and posters

New Generation Network; Special talk

Today's and Tomorrow's Challenges in Q Cryptography and Communication; Keynote 2

Q Cryptography

Assessment from modern cryptographer; Keynote 1

Past, Present, and Future; S3-2

Q Communication

Test of fundamental physics; Keynote 3

Engineering for telecom band; S5-2, P36

Theory; P11, 12

Optical Space Link; S5-4, S10-1, P47

QKD Field Network

Live Demonstration (Japan), Keynote 2 (Swiss), P33 (South Africa), P35 (China), P37 (Spain), P75 (China)

QKD Systems

Single photon; S2-1, 2, 3, 4, 5, 6

Entanglement; S2-6, S5-3, P39

Continuous variable; S5-1, S9-3, P43, P60

QKD Network Architecture; S2-6, S10-2

QKD Elements; P34, 38, 45

QKD Security

Analysis; S4-1, 4-2, P49, 50, 51, 52, 54, 57, 61

Side Channels and Countermeasures; S4-3, P40, 41, 42, 44

QKD Applications and Standardization; S10-3, 10-4, 10-5, P32

To widen a range of quantum cryptography

New Schemes of Secure Communications; P1, 2, 5, 48, 53, 55, 56, 58, 59

Toward scalable quantum networking

Quantum Repeater, Memory, and Media Conversion; S8-1, 8-2, 8-3, 8-4, 9-1, P15, 16

Optical Quantum Information Processing and Devices; S9-2, P3, 6, 13, 69

Foundations of quantum information technology

Photon Detection Technology
S6-1, 6-2, P10, 62, 63, 64, 65, 66, 71

Non-Classical Light Sources
P4, 46, 67, 68, 70, 72, 73, 74

Theory of Entanglement, Measurement, and Control; P7, 8, 9, 17, 18, 19, 20, 21

Quantum metrology gets closed to the real world

Optical Frequency Standard; S7-2, 7-3, P25, 30, 31

Quantum Technology with Atoms and Ions; S7-1, S7-4, P14, 22, 23, 24, 26, 27, 28, 29

Quantum cryptography

The viability of QKD is tested for practical use in the real world.

- **Speed and distance of QKD link**

  The Tokyo QKD Network made dramatic increase in secure bit rates, i.e., 300kbps with 4% QBER (Toshiba Research Europe), and 61kbps with 2% QBER (NEC-NICT) even under a high channel loss of 14.5dB at 45km, both used decoy-state BB84. They enabled one-time pad of movie data. At 90km (26dB loss) 2kbps secure bit rate was recorded using DPS-QKD (NTT-NICT). QKD is now realistic in a metropolitan area network.

- **Practical security guarantees**

  Like all security technologies also QKD has side-channels, i.e. gaps between the model for security proofs and its actual implementation. QKD needs a phase for identifying side-channels and patching loopholes for widespread acceptance.

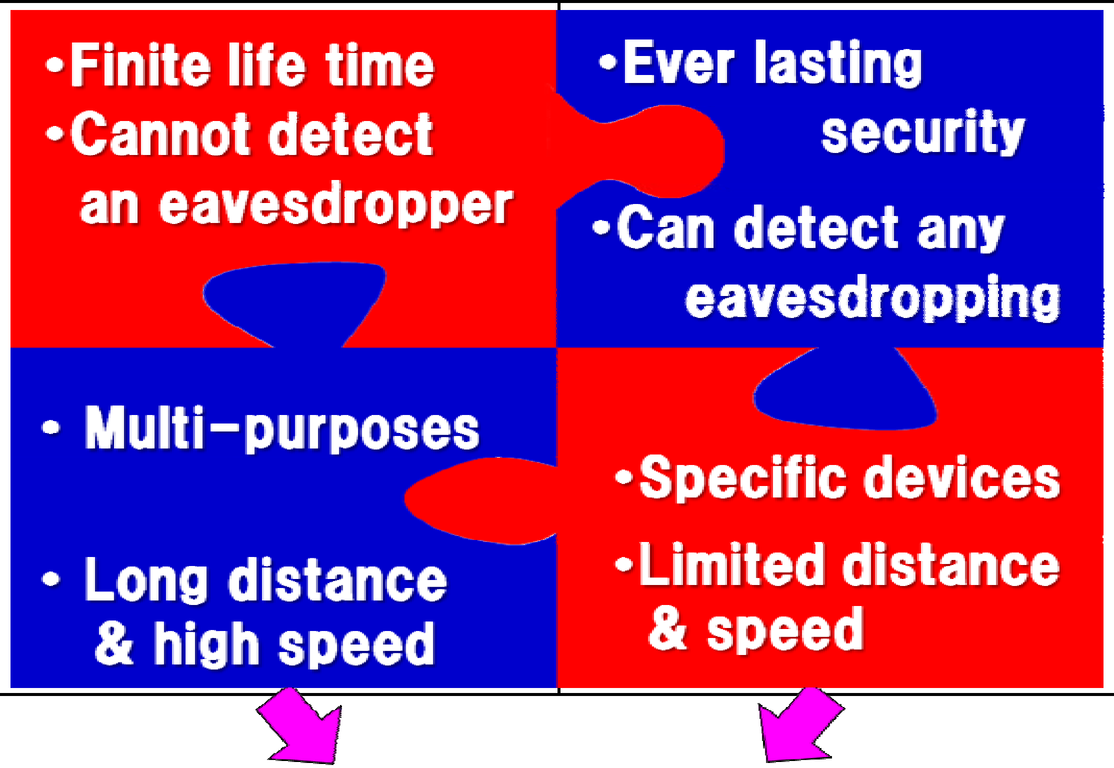
- **Research for new crypto-schemes**

  Compared with modern cryptography, current QKD schemes have many limitations. But at present we grasp only a small part of the possibilities that the merger of physics and modern cryptography will bring about. Challenges to find new amazing crypto-schemes have just started.

	Modern crypto	Quantum crypto
Key exchange	Public key crypto	QKD
Encryption/Decryption	Symmetric key crypto	One-time pad
	Algorithms of mathematics	Laws of physics

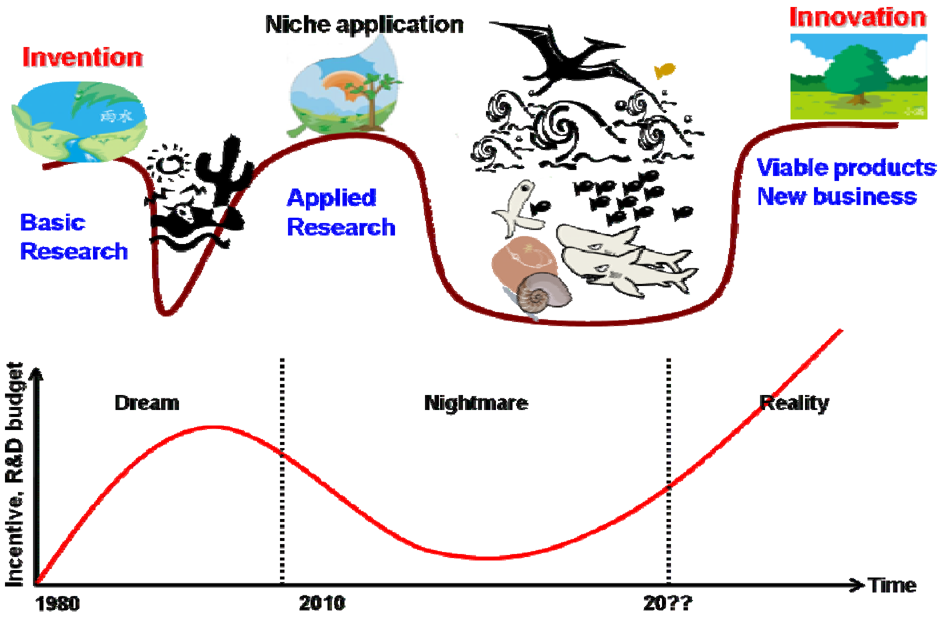
This table in the right presented by M. Sasaki on Day 1 was encouraging, however, may not be an adequate characterization of both schemes.

As discussed by A. Shamir, N. Gisin, other speakers and participants, the boarder is more subtle especially in terms of practical security.


•Finite life time
•Cannot detect an eavesdropper
•Ever lasting security
•Can detect any eavesdropping
• Multi-purposes
• Long distance & high speed
•Specific devices
•Limited distance & speed

Should be combined to serve for realizing the safe and secure society

Current status : QKD may have crossed the Valley of Death, and now gets into the Darwinian Sea….



There are at least two deep valleys in a route from invention to innovation. One is the Valley of Death from basic research to applied research. There are still risks for enterprises. Even if one can luckily overcome this valley, one often gets into the Darwinian sea, where further Struggle for Life of technological and entrepreneurship risks goes on. Technological limitations to impede industrialization become evident. Resistance from existing scheme becomes apparent and disappointment spreads. It is a stage of nightmare. QKD may have crossed the Valley of Death, and now gets into the Darwinian Sea.

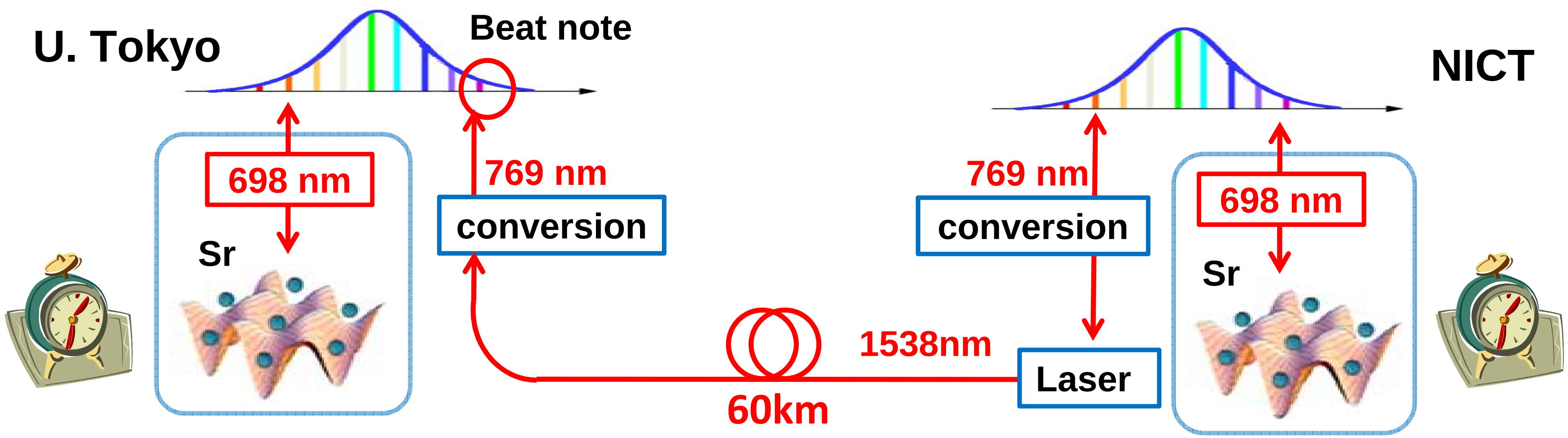
Although some companies and organizations have started to use QKD daily for good reasons, the market is, however, still niche. To survive in the Darwinian Sea, we should listen humbly to the assessment from modern cryptographer and have much more dialogue with potential users. Deepening QKD and related technologies is necessary, but not sufficient at all. In this phase we should employ all scientific knowledge and technologies in the relevant fields by a cross-disciplinary approach, and should reinvent killer methods and new applications. The QKD technology will then become reality in real world.

Quantum metrology

- Synchronization of Sr optical lattice clocks through an optical fiber

Real-time comparison in the *15th digit* over 60km distance

f = 429228004229874Hz



- Much improvement on the averaging time. Conventional scheme with satellite microwave communications takes a day.

- Related technologies of optical lattice and trapped atoms/ions will realize quantum simulation and ultra-precise magnetometry.

Quantum networking

Impressive experimental and theoretical progress has been reported.

- **The 4-Layer architecture for fault-tolerant quantum repeaters was proposed. Various constituent technologies in the physical layers with optically controlled semiconductor quantum dots were presented.**

- **Workable quantum memories can be built in the near future.**

  Photon-echo quantum memory with rare-earth-ion doped crystals;
  - Controlled Reversible Inhomogeneous Broadening (CRIB)
  - Atomic Frequency Comb (AFC)

  Non-classical storage of entangled photons was reported.
  The storage bandwidth was widened to >1 GHz.

- **Quantum media conversion**
  The spin state transfer between light and electrons in a GaAs/AlGaAs semiconductor were presented.

Optical quantum information technology

- Impressive progress in integrated quantum photonic circuits and non-classical light sources has been reported. The integrated quantum photonic circuits will be performing calculations that are outside the capabilities of conventional computers in the near future.

- Remarkable improvement was achieved in semiconductor single photon detectors thanks to state-of-the-art readout technology.
  Clock rate and detection efficiency were increased up to 2GHz and 20% respectively. It enabled the fastest QKD under a high channel loss of 14.5dB at 45km (--> S2-5).
  Reduction of dark counts and after-pulse effect are main obstacle.

- Superconducting single photon detectors (SSPDs) have low dark counts and no after-pulses. Detection efficiency is rapidly improving, and will be >50% in the near future.
  SSPD is only the solution at present to realize long distance QKD (--> S2-3, S5-3).