ATIP Report: Insights from QCrypt 2015, Tokyo

ATIP/Japan

ABSTRACT: The 5th International Conference on Quantum Cryptography (QCrypt 2015) was held in Tokyo from September 28 - October 2, 2015. This annual international conference focuses on quantum cryptography and its applications for secure communications, including experimental and theoretical works. Topics include quantum communications using quantum key distribution (QKD) networks, either optical fiber, free-space, or via satellite, as well as issues regarding the level of security quantum networks have against untrusted parties or attacks. The need for "post-quantum" cryptography or "quantum safe" schemes is also discussed. QCrypt 2015 was prefaced by the half-day Updating Quantum Cryptography and Communications conference (UQCC 2015), which showcased the progress of the large UQCC project in Japan that is developing the next-generation of the Tokyo QKD Network. Japan was not the only focus of UQCC - the conference also included international collaborators to gather their perspectives in this area. The present report provides an overview of the conference, including research highlights, trends, and important insights from the top researchers in the field. Details on important status updates of the Tokyo quantum network are also included.

KEYWORDS: Defense Applications, Information Technology / IT, Mathematics, Photonics / Optoelectronics, Physics, Quantum Information S&T / QuIST, Space / Satellite /Aerospace, Telecommunications / Networking

COUNTRY: Japan

DATE: November 24, 2015

REPORT CONTENTS

1. INTRODUCTION

The 5th International Conference on Quantum Cryptography (QCrypt 2015) was held in Tokyo from September 28 - October 2, 2015. This annual international conference focuses on quantum cryptography and its applications for secure communications, including experimental and theoretical works. Topics include quantum communications using quantum key distribution (QKD) networks, either optical fiber, free-space, or via satellite, as well as issues regarding the level of security quantum networks have against untrusted parties or attacks. The need for "post-quantum" cryptography or "quantum safe" schemes is also discussed.

QCrypt 2015 was prefaced by the half-day Updating Quantum Cryptography and Communications conference (UQCC 2015), which showcased the progress of the large UQCC project in Japan that is developing the next-generation of the Tokyo QKD Network. Japan was not the only focus of UQCC - the conference also included international collaborators to gather their perspectives in this area.

The present report provides an overview of the conference, including research highlights, trends, and important insights from the top researchers in the field. Details on important status updates of the Tokyo quantum network are also included.

EXECUTIVE SUMMARY

- Every day, public-key encryption and digital signatures such as RSA protect billions of Internet communications and transactions. If today's encryption were to be broken by quantum computers, it would have a devastating impact on world commerce and communications.
- It was commented on that a big shift in perspective for the whole quantum cryptography field since 2014 is the announcement in August 2015 by the US National Security Agency (NSA) of preliminary plans for transitioning to quantum resistant algorithms - that is, systems that will be secure even if quantum computers are available to break existing cryptography. If NSA is preparing for a world with quantum computing, then others will follow, so the shift in perspective is that the "quantum era" has started, and now is the time for quantum cryptography or "quantum-safe" schemes to "show its stuff." Comments were also made that this basically means "RSA is *de facto* dead" - something that would not have been said in 2014.
- Given NSA's announcement, Michele MOSCA of The University of Waterloo in Canada suggests that in the next 6-24 months, those organizations without a well-articulated quantum risk management plan will lose business to those who do.

  MOSCA also warned that it takes time to prepare for such a quantum world, as he illustrated in Figure 1 below. It is hoped that the time (y) to prepare "quantum -safe" schemes is shorter than the time it takes for quantum computers to be readily realized (z). Given the continued developments toward quantum computing, he and others suggested it is "almost time to panic."

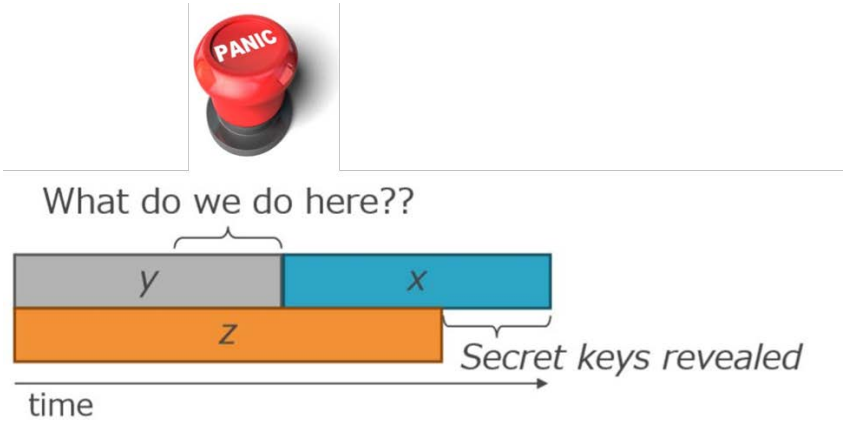

Figure 1. How much time before you have to worry about a world with quantum computers? You need to hope the time (y) for you to prepare "quantum -safe" schemes is shorter than the time it takes for quantum computers to be readily realized (z), and the time you want your secret keys secure (x).

(Source: Michele MOSCA, University of Waterloo)

Even though how large a quantum system (qubits) would be needed to break the existing RSA-2048 encryption still has not been defined, MOSCA predicts a 1 in 7 chance of breaking RSA-2048 by 2026, and a 1 in 2 chance by 2031. Thus, he calls it a "medium term threat."

- On a more philosophical note, MOSCA also suggested that Shor's algorithm, formulated in 1994, was an "historical fluke," that was luckily discovered before quantum computers

existed. Therefore, it should be used as a warning to prepare for the day when quantum computers are available. Shor's algorithm, if used on a quantum computer, can factor large numbers and will thus be able to break public-key cryptography such as the widely used RSA. In the past 15 years, several groups have realized Shor's algorithm for factoring in primitive systems of several qubits, suggesting there may not be too much time before usable quantum computing systems are realized.

- MOSCA's offered the following suggestions for industry and government:
  1) Get quantum-safe options on vendor roadmaps (routinely ask about vulnerability, include quantum-safe options as desired features).
  2) Make quantum risk management a part of their cybersecurity roadmap.
  3) Request information/studies needed to make wise decisions.
  4) Applaud and reward organizations that take this seriously.
- Several people referred to the development timeline for a quantum computer originally created by R. SCHOELKOPF of Yale University in 2013 (Figure 2). In recent years there have been demonstrations of longer lifetimes in qubits (superconducting, diamond NV centers, Si qubits, ion traps etc.), so development is currently at the fourth step and researchers are trying out operations on the fifth step in Figure 2. Some are also trying fault-tolerant computing with surface code schemes for error correction. Again, the point being that quantum computing may not be that far away.

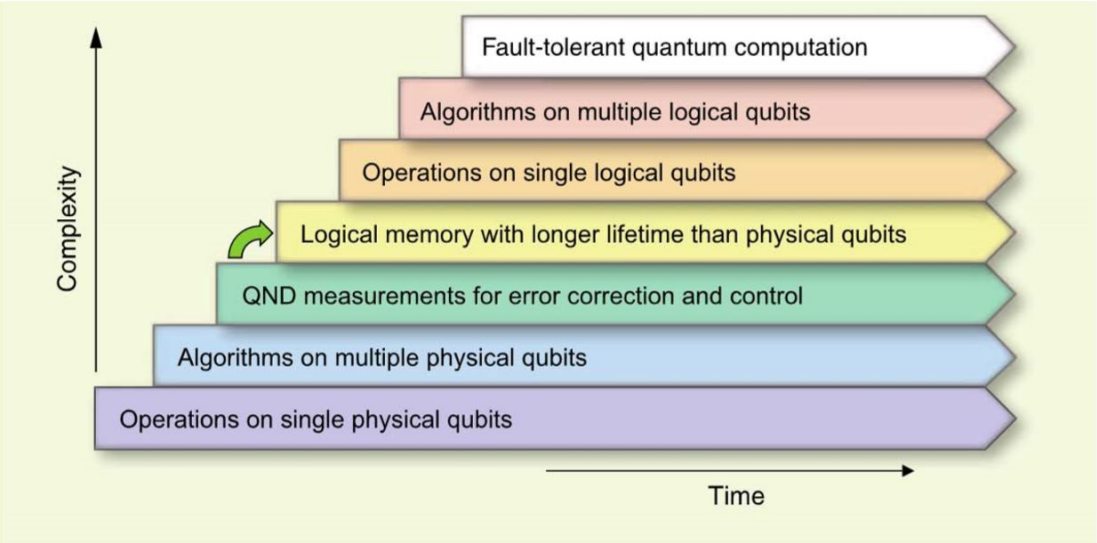

Figure 2. Seven stages in the development of quantum information processing. Originally from R. SCHOELKOPF (Yale University) showing the position (step 3) in 2013. In 2015, we are now around step 4-5.

- However, there were also some more subdued tones expressed at the conference. Some participants suggested that QKD has 10 years (not 20 years) to prove itself and find its market, or it will be dead and replaced by some other scheme. The reality, though, is that QKD will still be needed in 10 years if no better alternative scheme is found. There are QKD networks for research in the US, Europe, Japan, China, and Korea; however, these networks may have only about 10 years to prove themselves and to be broadened for practical use by governments and financial institutions, etc.

- Another issue for QKD is that the existing IT players are not interested in it, as it requires new systems, new ways of doing things, and they don't fully understand it. Also, the existing security measures are considered to be "good enough" for now. This attitude is shown in Figure 3, which represents a slide that the company Cisco has shown elsewhere suggesting QKD is not needed. Some people suggest that the real requirements from the market are even more severe than that. It is somewhat of an "apples vs. oranges" comparison, but shows that QKD has tough barriers to overcome, with legacy systems and players.

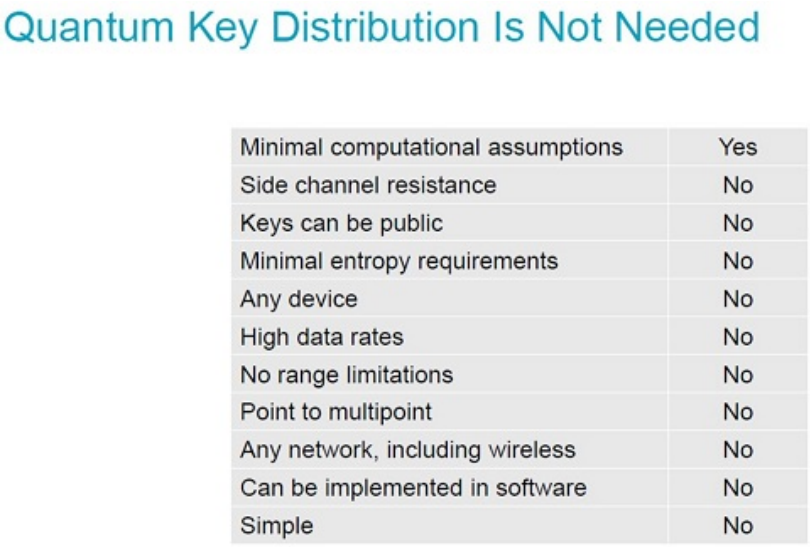

Figure 3. An image that Cisco has shown elsewhere, suggesting QKD is not necessary

- One complaint of QKD is that it is slow. However, several groups have demonstrated that it will be possible to have secret key rates over gigabits per second (Gbps) in the very near future. It was also highlighted that QKD is not necessarily slow compared to what is used now on existing OpenSSL servers, where key generation can be on the order of 256 kb/sec. Operators are not complaining about the speed of these schemes, which is comparable to the speed of the existing QKD.
- Another issue with the quantum cryptography field is that traditional cryptographers do not want to deal with quantum. Maybe their understanding is limited, and they feel more comfortable with systems they are familiar with and believe are "good enough." For example, attendance at the QCrypt conference has been dominated by physicists and virtually no traditional cryptographers.
- For the time when quantum computers are readily available, the discussion becomes centered on this question: What is "Quantum-safe" cryptography that is resistant to quantum attacks? There are two schemes that are currently being contemplated:

  1) Quantum cryptography: Based on truly random numbers and QKD.
     - Characteristics: Provably secure, backward security, expensive, big change in infrastructure & mentality.
  2) Post-quantum cryptography: Complexity-based classical algorithms (e.g., lattice, multivariate, etc.) that are deployable without quantum technology.

- Characteristics: Not much change for security experts, vulnerable backwards, believed/hoped to be secure against quantum attacks of the future.

At this stage, all that can be said is that each will likely find some applications, or they could be used in combination.

- The 20th Century involved "security by inaccessibility," which was achieved by locking information up. In contrast, the ideal behind quantum communications for the 21st Century is "security with accessibility" – that is, systems are open, but the ultimate security is based on quantum systems.
- There are several QKD networks around the world, and some developments were highlighted at QCrypt as follows:

❖ **JAPAN**

Optical Fiber	The Tokyo QKD Network is a 45-km (90-km loop) intra-city network used as an open test-bed for next-generation QKD equipment. Its developers hope to get government or financial users to use it in the next 5-10 years.
Free Space	8-km test-bed in Tokyo
Satellite	Ground-to-satellite laser quantum communications testing with the SOCRATES satellite. Another satellite is planned for 2016. A Japan relay network is being planned for 2019.

Separately, Toshiba has been trailing a QKD network for secure transmission of genomic information and medical records over a distance of 7 km from a genetics analysis center to a genetics databank since August 2015.

The Japanese have also developed a system with quantum secure keys to give medical record access to certain people, which could be used within and between hospitals.

One indelible image of the conference is it that of quantum entanglement in a "quantum car," using QKD inside the car for secure communications and control between the vehicle's driving systems. Proposed by the Japanese, this seems at first glance to be a little overboard in terms of an application. However, considering the implications, particularly for autonomous driving, this is one life-or-death application that would require the ultimate in systems that are secure and safe from hacking or corruption. This application is still a long way from actual realization, though.

- **CHINA**

Optical Fiber	• Heifei Intracity Quantum network: 46 nodes. • Jinan quantum communications network: 50 nodes, 28 institutions, and 90 users over a 70-km^2 area. • 2000-km QKD network planned between Beijing and Shanghai, via Heifei and Jinan. Will need quantum repeaters, but first will prepare networks in the four cities.
Satellite	Quantum science satellite will be launched around 2016, led by Prof. Jian-Weui PAN of the University of Science and Technology of China (USTC). Collaboration with the European Space Agency and University of Vienna in Austria.

- **VIENNA**

Optical Fiber	SECOQC QKD network in Vienna between institutions.
Free Space	Demonstrated QKD over 144 km in the Canary Islands. Also, a 3-km test-bed in Vienna.
Satellite	Collaborating with USTC in China.

- **US:**

Optical Fiber	The research organization Battelle has a QKD test-bed loop (4x110km, 8x25km) in Columbus, Ohio providing >400 km network. Using ID Quantique QKD equipment.

- **ITALY:**

Satellite	University of Padova is doing research on ground-to-satellite quantum communications.

- There were a number of technical announcements made at QCrypt regarding improvements in QKD networks, including:
  1) Distance improvements: Distances over 300km.
  2) Rate improvements: Speeds over 1-Gbps should be possible.
  3) Repeaters: Without repeaters, QKD is limited to around 400km. The problem with repeaters is that they need quantum memories, which are difficult. There have been continued developments in this area, such as proposals for an all-photonics repeater that does not require memories.
  4) Device-independent QKD: Measures to address its slow speed.
  5) Photon detectors and sources: Improved components have shown improved network performance.

IMPACT & ASSESSMENT

A big shift in the perspective occurred in the field of quantum communications within the past year, as the US NSA announced plans to transition to quantum resistant algorithms. Others will follow, so there will be increased pressure to consider quantum risk, leading to the beginning of the "quantum era."

It is likely to be many years (maybe 10-20?) before robust, large, and usable quantum computers are available, if at all feasible. However, it will also take time to prepare for such a world where "quantum-safe" systems will be needed that will be secure even if quantum computers are available to break existing cryptography such as RSA.

Post-quantum cryptography is showing some promise, and is more similar to traditional cryptography, while QKD provides ultimate security but needs new infrastructure. It is still too early to say, but both QKD and post-quantum cryptography may find areas of use. However, with legacy IT system vendors and the traditional cryptography community showing little or no interest in or understanding of quantum technologies what will happen when the time to become "quantum-safe," becomes an urgent necessity? From ATIP's perspective, if post-quantum cryptography shows real viability, then it may be an easier leap for the legacy people and IT vendors.

2. QCRYPT 2015 HIGHLIGHTS

Details of the program, including abstracts and a list of posters, are included as a separate file accompanying this report as Appendix A. The conference presentation slides and posters are also included as Appendix B, which will be provided separately on USB. Including the UQCC event, there were 334 participants overall; 277 attendees from 24 countries participated in QCrypt, as shown in Figure 2.1. A partial list of participants is included at the end of this report as Appendix C. QCrypt participants are mostly physicists or mathematical physicists rather than traditional cryptographers.

Since the key messages of the conference are covered in the Executive Summary above, they will not be repeated here. This section provides further details on some of the highlights of QCrypt 2015.

Figure 2.1. QCrypt 2015 participants

2.1 Post-Quantum Cryptography

For the time when quantum computers are readily available and can break existing encryption such as RSA (Figure 2.2), a "Quantum-safe" cryptography that is resistant to quantum attacks will be required. Besides quantum cryptography based on QKD to send secure keys, post-quantum cryptography also has the potential to meet this need.

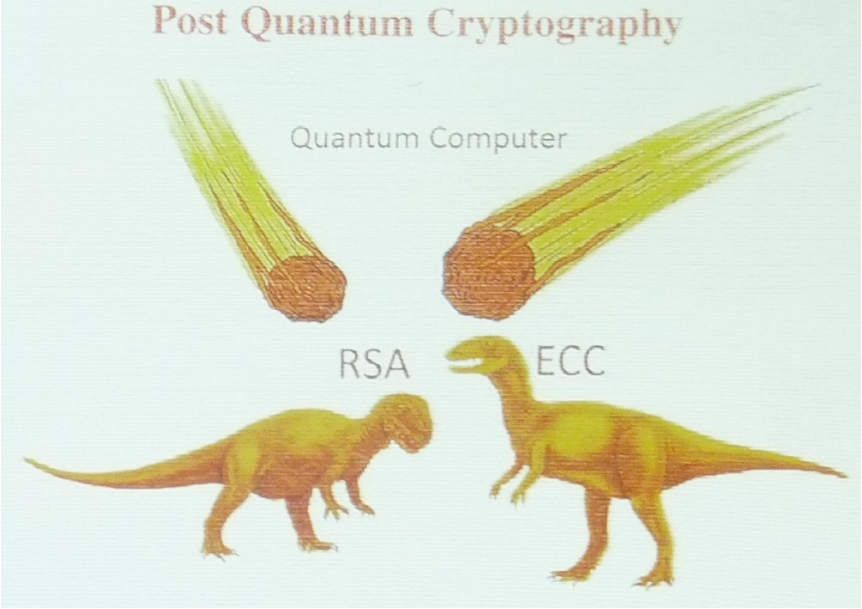

Figure 2.2. Image portraying the future of existing encryption, such as RSA, when quantum computing is realized

As a leader in this area, Johannes BUCHMANN of TU Darmstadt in Germany described that post-quantum cryptography requires coming up with algorithmic problems that are hard even with a quantum computer, and at the same time, can be the basis of public-key cryptography. There are presently four types of such problems that are promising:

1) Lattice problems: security based on the hardness of finding short or close vectors in a lattice.
2) Multivariate problems: based on hardness of solving systems of non-linear multivariate equations.
3) Code-based: Based on hardness of decoding linear codes.
4) Hash-based signatures: based on hardness of finding collisions of cryptographic hash functions.

Hash-based signatures and code-based public-key encryption are the most advanced at this stage. Lattice-based cryptography is very interesting and promising, but it still needs more investigation. Multivariate cryptography is interesting because it allows for extremely efficient realizations in hardware such as smart cards, for example. Again, more investigation is needed.

Post-quantum cryptography is characterized by:

- Not much change for security experts, as it still involves solving a problem.
- Vulnerable backwards.
- Believed/hoped to be secure against quantum attacks of the future.

However, post-quantum cryptography is not guaranteed to resist quantum computer attacks, so in that way it is similar to existing encryption schemes. Meanwhile, for quantum

cryptography based on QKD - it is unclear whether it can implement public-key cryptography and signatures, so it may not replace classical public-key cryptography.

So ultimately, a combination of classical and quantum cryptography may be needed to achieve the required security. QKD's strength is that it can protect exchanged keys forever, so it can be the basis for protecting data in transmission. At the same time, such communications also require proofs of authenticity. Such proofs only need to be verified for a short while, when the communication actually happens. Therefore, QKD together with post-quantum signatures may provide the required security.

Separately, there was mention at the conference of standardization bodies looking into "Quantum-safe" issues (Figure 2.3). The European Telecommunications Standards Institute (ETSI) in Europe has a telecommunications focus, and is thus looking at QKD standardization. The Cloud Security Alliance (CSA) is a more IT vendor-focused group that also has a quantum-safe working group. Standards will be important for interoperability, integration in conventional networks, stimulating the development of common interfaces, and thus stimulating component supply.

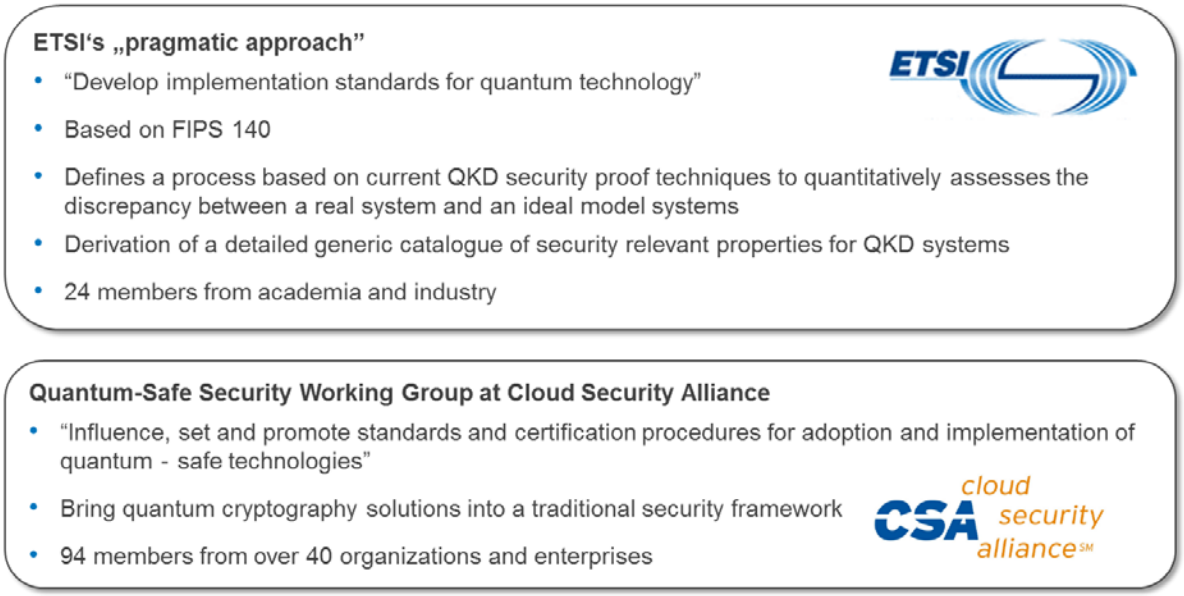

Figure 2.3. ESTI and CSA have groups looking into quantum-safe issues and standardization

2.2 Security Attacks on Quantum Key Distribution (QKD)

The security of QKD can be mathematically proven, but it is still vulnerable to "side-channel attacks" such as blinding the photon detector. Prof. Akihisa TOMITA of Hokkaido University in Japan reviewed the methods of such attacks (Figure 2.4), as well as what type of system design and monitoring is needed to prevent such attacks (Figure 2.5).

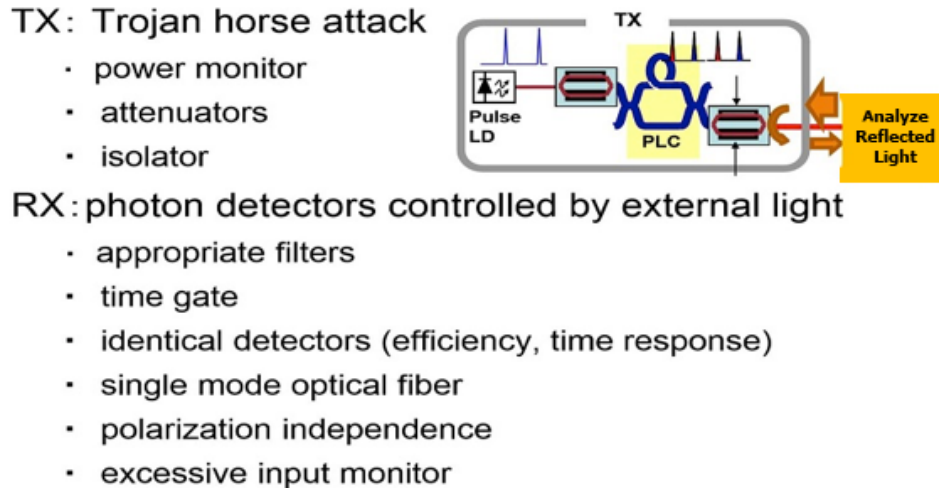

Figure 2.4. Some of the side-channel attacks possible in QKD systems

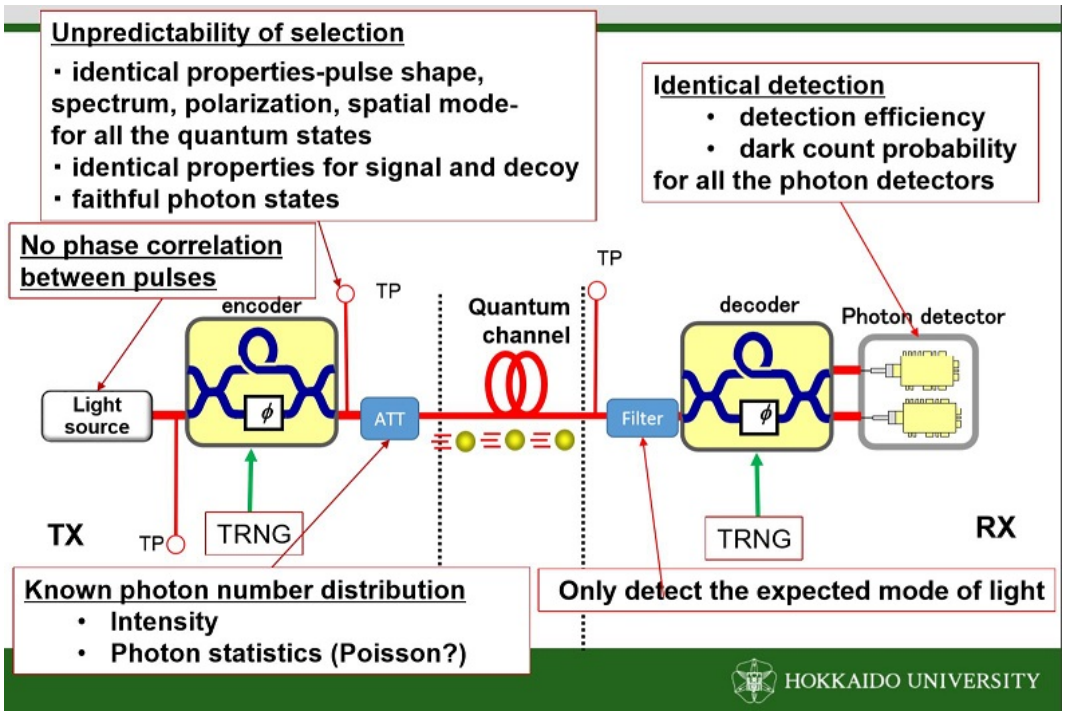

Figure 2.5. Requirements for QKD equipment to reduce possibility of side-channel attacks

To help overcome some of the issues, "Device Independent QKD" has been previously proposed to realize perfect security, even when the internal working of the device is unknown or the provider is not trusted. This would also help in opening up the market, as components would be supplied by a number of different providers and it is not easy to certify every component for perfect security.

However, implementing device independent QKD has resulted in very low secret key rates so far. Hugo ZBINDEN's group at The University of Geneva looked at where researchers have attacked QKD systems (see Figure 2.6, for example) and saw that in most attacks, the

weakest part of QKD seems to be at the photon detector. ZBINDEN et al. proposed and demonstrated "detection device independent QKD," which is a simpler alternative to device independent QKD and gives faster performance.

Attack	Target component	Tested system
Time-shift	Detector	Commercial
Time-information	Detector	Research
Detector control	Detector	Commercial, research
Detector dead time	Detector	Research
Channel calibration	Detector	Commercial
Phase remapping	Phase modulator	Commercial
Faraday Mirror	Faraday mirror	Theory
Wavelength	Beamsplitter	Theory
Phase information	Source	Research
Device calibration	Local oscillator	Research

Figure 2.6. A list of possible attacks on QKD systems, showing that many are focused on the detector *(Source: TAMAKI et al.)*

2.3 QKD Network Developments Around the World

Worldwide, there is presently a number of QKD networks being trialed and several more under development (Figure 2.7). At QCrypt 2015 and UQCC 2015, several groups gave updates on their developments as shown below.

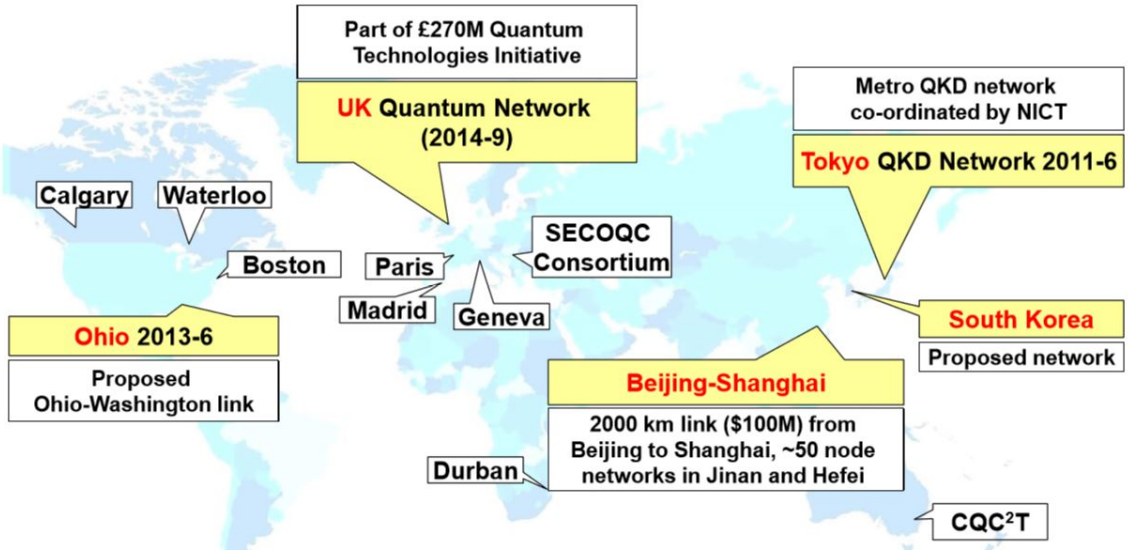

Figure 2.7. Implemented test-bed QKD Networks and those planned

2.3.1 Japan QKD Network Developments

The Tokyo QKD Network is a 45-km (90-km loop) intra-city network (Figure 2.8) that was inaugurated in 2010 and used as a research test-bed. It has demonstrated secure QKD

network operations, including absolutely secure video transmission, detection of an eavesdropper, and rerouting to secondary secure links. The network has also shown stable, maintenance-free, continuous operation for periods of 30 days or longer. As new technologies are developed, they are trialed in this Tokyo QKD network.

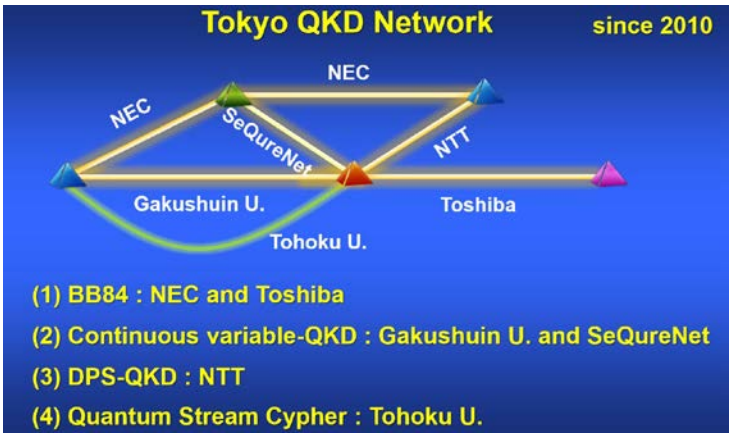

Figure 2.8. The Tokyo QKD Network has a 45km backbone (90 km loop). Also shown are the partners working on various next-generation components who trial them on segments of the network.

The Tokyo QKD Network development efforts started in 2001 under the UQCC project, with initial implementation and continual updating since then. The UQCC project is coordinated by Japan's National Institute of Information and Communications Technology (NICT), and NICT commissions component development to various companies and institutions (see Figure 2.9 below)

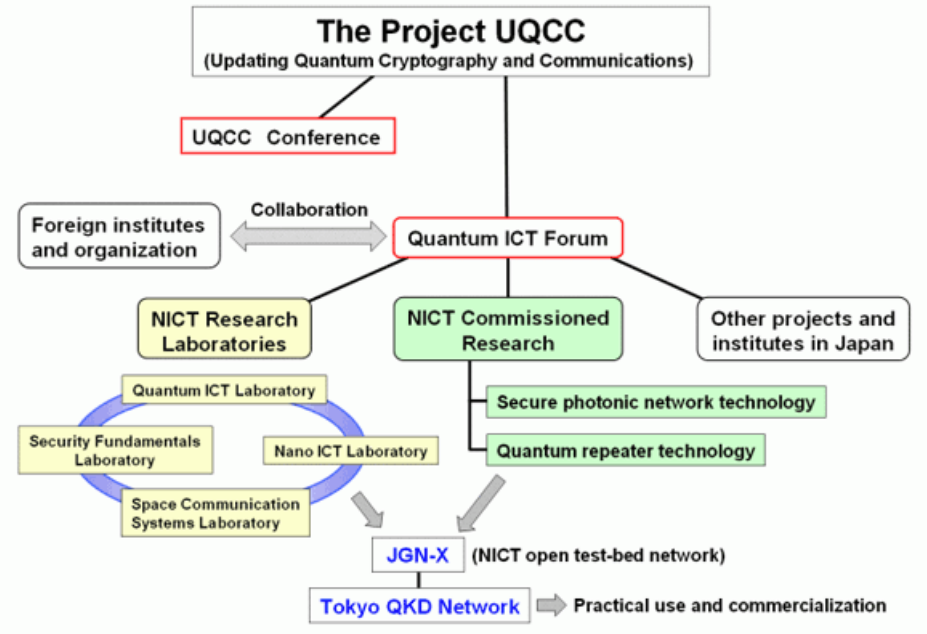

Figure 2.9. Organization of UQCC program based in NICT

From its inception in 2001, the UQCC project is nearing the end of Phase III (2011-2016) with funding on the order of US$25-30M over this phase. Since Phase III will end in March

2016, the work will continue under the newly started (2014-2019) IMPACT project, which includes a "Quantum Secure Network" sub-project (US$9.2M over a period of five years) to be run by NICT, which will continue developing the technologies and components and implementing them into the Tokyo QKD network.

The timeline shown in Figure 2.10 below illustrates the goals of the UQCC program, with the following as Phase III goals:

1. To make practical use cases of a quantum cryptographic network.
2. To develop quantum node technologies for a quantum communications network.
3. To apply techniques and devices developed in those researches to new sensing technologies and metrology.

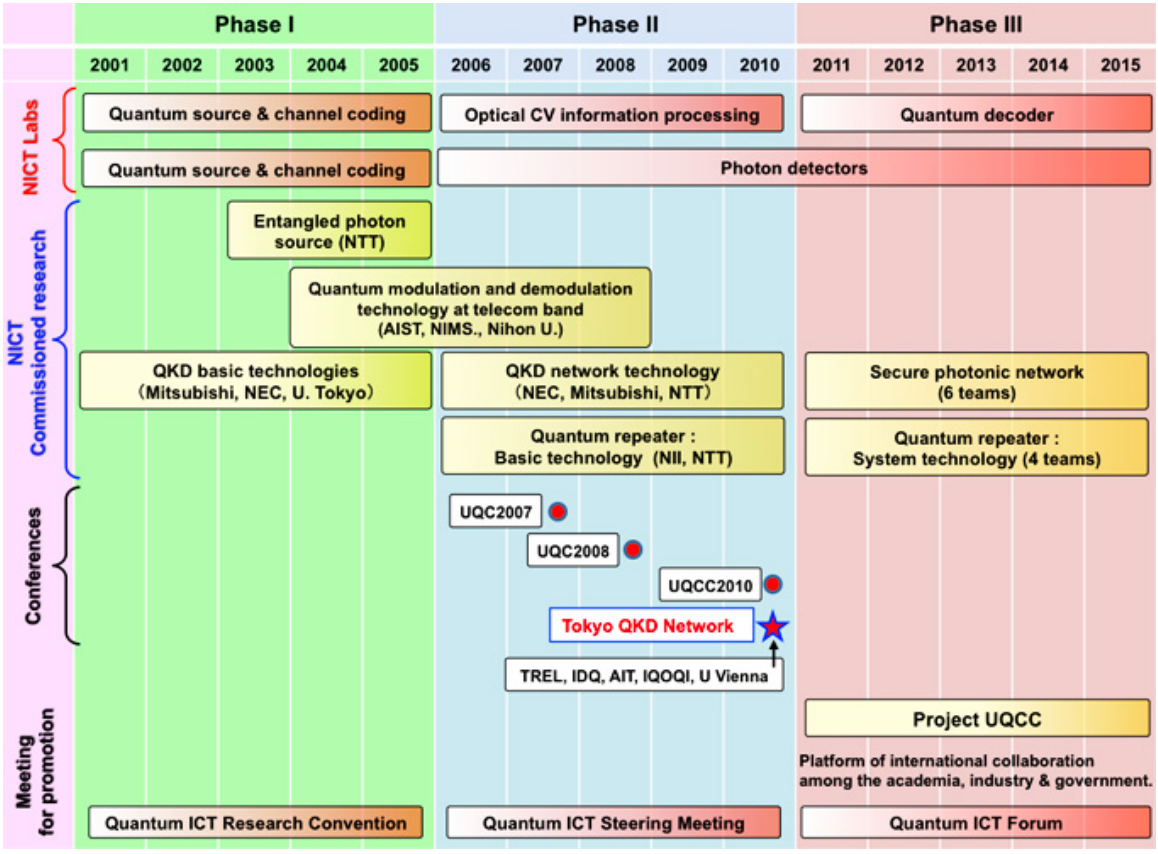

Figure 2.10. Schedule of the UQCC program, presently in Phase III

NICT's Commissioned Research Program has the following three main goals:

1. Develop a QKD system for metropolitan IP networks within a 50-km range at a minimum key generation rate of 1 Mbps. Networking and WDM technology will also be applied.
2. Construct a QKD system exceeding the 100-km range at a key generation rate of 10 kbps or higher.

3. Develop basic hardware for a quantum repeater using NII and NTT. Nuclear spins and electron spins in solids will be exploited for scalability, and entanglement swapping will be demonstrated.

Phase III of the UQCC program (2011-2016), to improve secure quantum networks, is in its last year - so there are deadlines from the original schedule. From developments over the past year, it appears that some of the next-generation components are finally coming together. For example, integrating NICT's own single-photon sources and single-photon detectors into the network have shown improvements in quantum network performance, up to 1,000 times better in some cases.

However better single-photon sources are still a bottleneck. Meanwhile, with quantum repeaters, which are needed for long-distance communications, there are various possible physical schemes, each with potential but each of which may not be ready by the end of Phase III of the UQCC program.

The more detailed roadmap shown in Figure 2.11 below illustrates how next-generation QKD technologies and components are trialed in the Tokyo QKD network as they are developed by the partners. For 2016-2020, they wish to trial the network as a service to users who need absolutely secure networks, such as governments, financial institutions and medical organizations (see Figure 2.11 below).

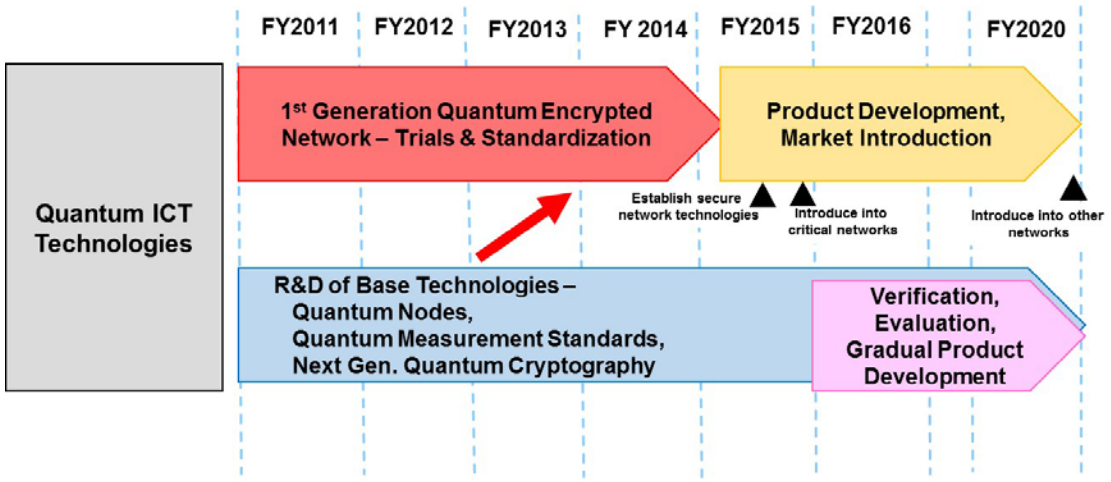

Figure 2.11. Quantum communications research roadmap followed by the UQCC program by Ministry of Internal Affairs and Communications (MIC)

NICT has been discussing with the Japanese government for the past two to three years on possibly using the QKD network. The government is still watching the situation, but one issue is that the traditional communications people do not fully understand the new quantum technologies or what they are capable of. For example, traditional radio frequency (RF) specialists did not initially understand quantum communications, but since they were shown how to use quantum systems, their level of interest has increased.

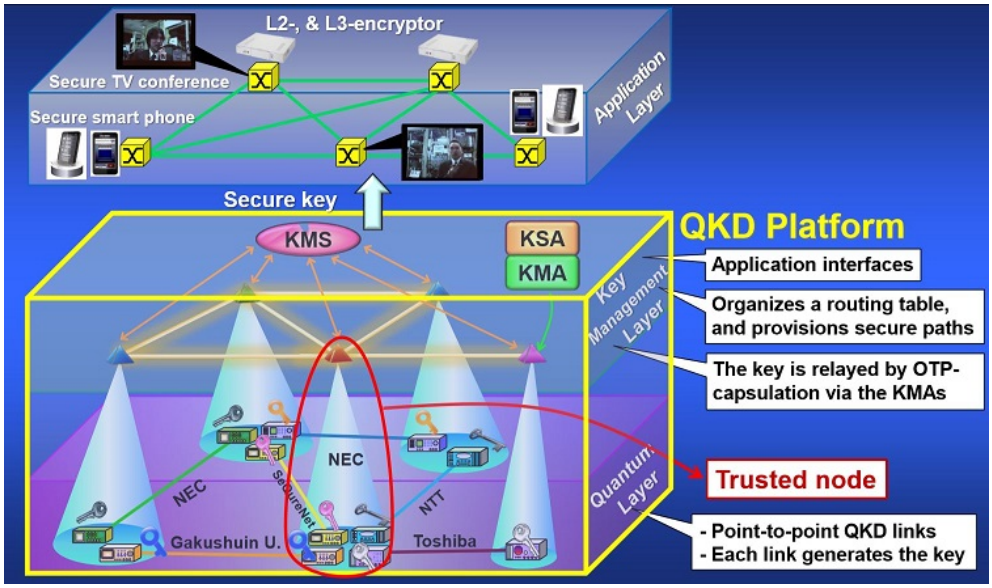

Figure 2.12. The hierarchy of the Tokyo QKD platform based on secure quantum technology (bottom) to provide secure services (top)

Using the Tokyo QKD network and technologies, partners have been developing and demonstrating applications on the network, which will be highlighted below. For example, Mitsubishi Electric has previously demonstrated secure mobile phone communications using the QKD network for secure key transmission (Figure 2.13). NEC has also done similar (Figure 2.14)

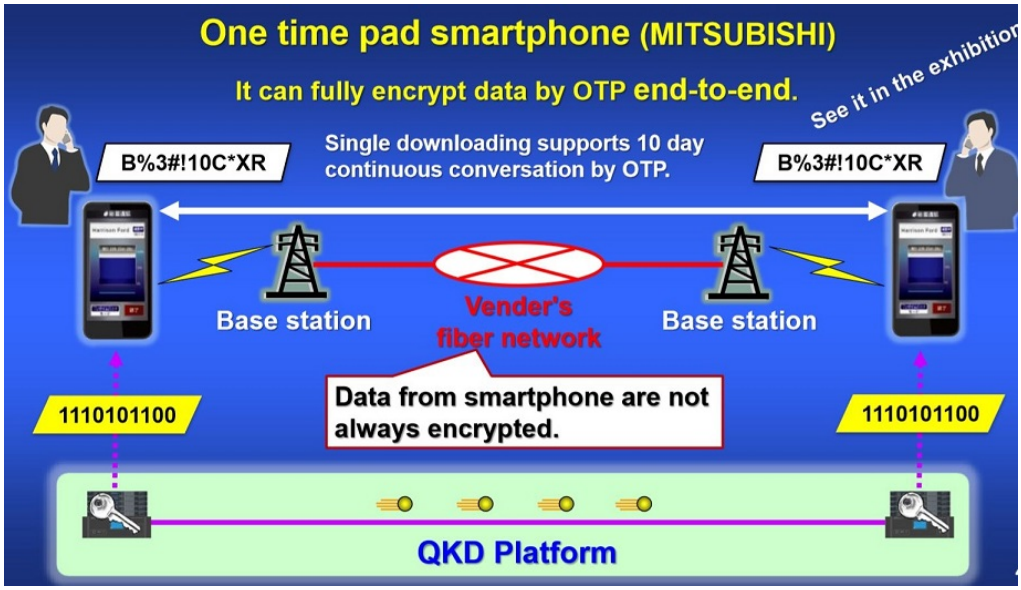

Figure 2.13. Mitsubishi Electric has demonstrated secure mobile phone communications with secure key transmitted by QKD network

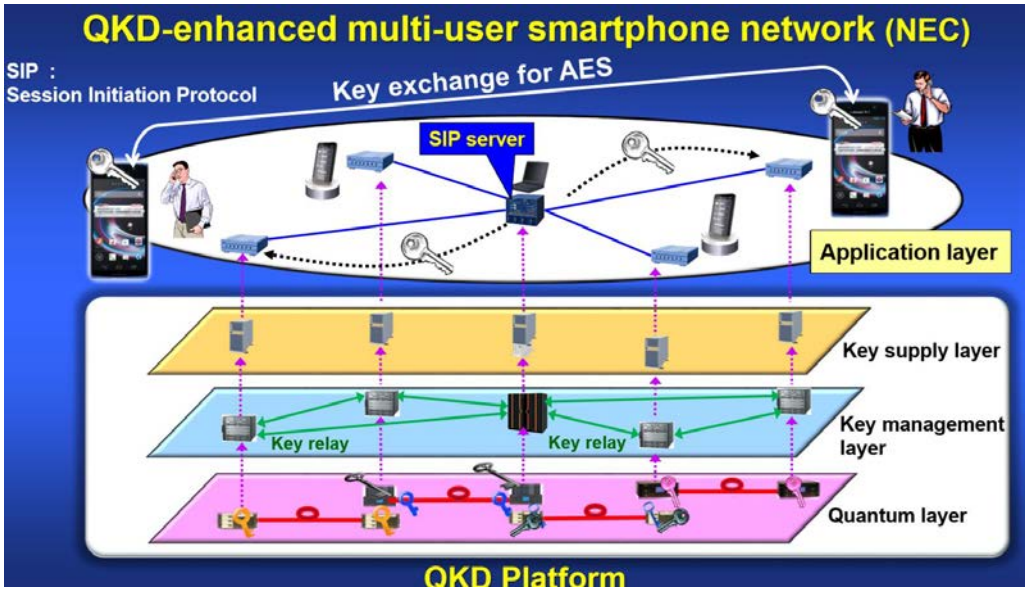

Figure 2.14. NEC's scheme for secure mobile phone communications with secure key transmitted by QKD network

As mentioned earlier, Toshiba has been trailing a QKD network for secure transmission of genomic information and medical records over 7km from a genetics analysis center to a genetics databank since August 2015, as illustrated in Figure 2.15.

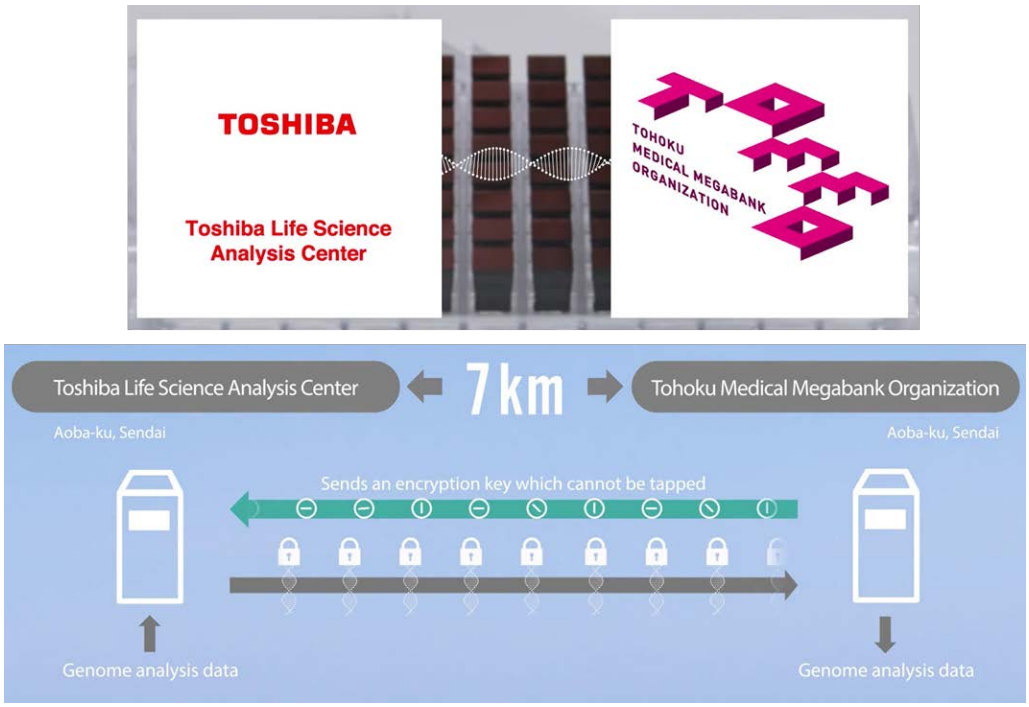

Figure 2.15. Toshiba has been trailing a QKD network for secure transmission of genomic information from a genetics analysis center to a genetics databank

The Japanese have also developed a system with quantum secure keys to give medical record access to certain people that could be used in and between hospitals, as illustrated

in Figure 2.16. This system was actually demonstrated in a skit on stage by the world famous cryptographers, Gilles BRASSARD and Charles BENNETT, playing doctor and patient. NICT has also demonstrated secure communications with drones, using QKD for secure keys (Figure 2.17).

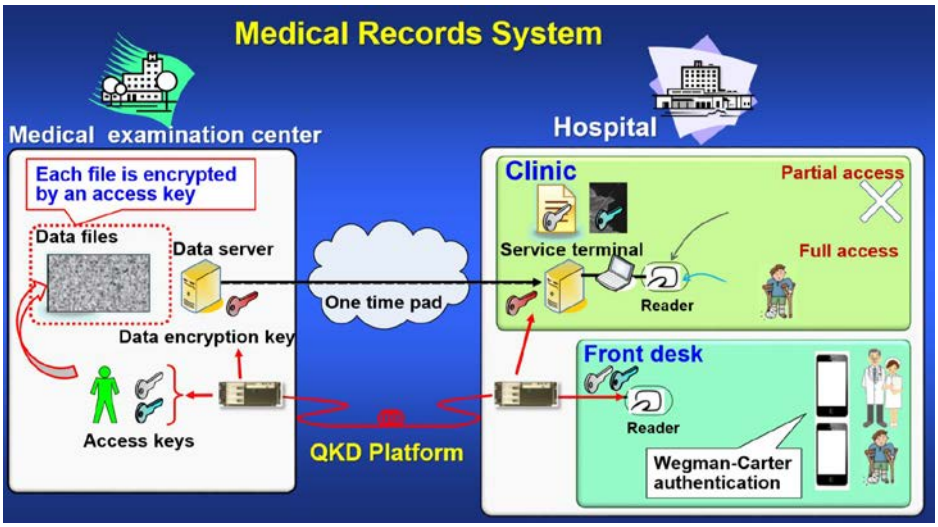

Figure 2.16. System for secure transfer and access to medical records

Figure 2.17. Demonstration of secure communications between drones (above), and how keys can be passed along as the drone travels over various regions (below)

One indelible image of the conference was that of quantum entanglement in a "quantum car," using QKD inside the car for secure communications and control between the cars driving systems (Figure 2.18). Proposed by the Japanese, this at first it seems a little overboard in terms of an application; however, considering the implications, especially for autonomous driving, it is one life-or-death application where systems with the ultimate security and safety from hacking or corruption would be required. This application is a long way from actual realization, though. Another possible use of QKD networks is in storage area networks (Figure 2.19).

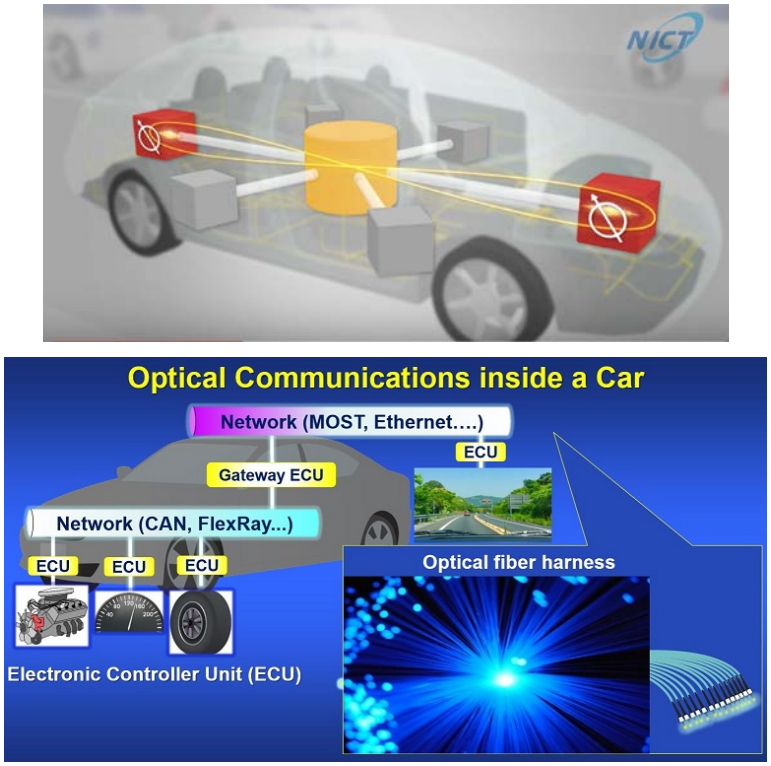

Figure 2.18. A typical car has many internal networks between driving systems (bottom image), and would include autonomous driving systems in the future. An image of quantum entanglement in a car that would give secure communications between such systems (top image).

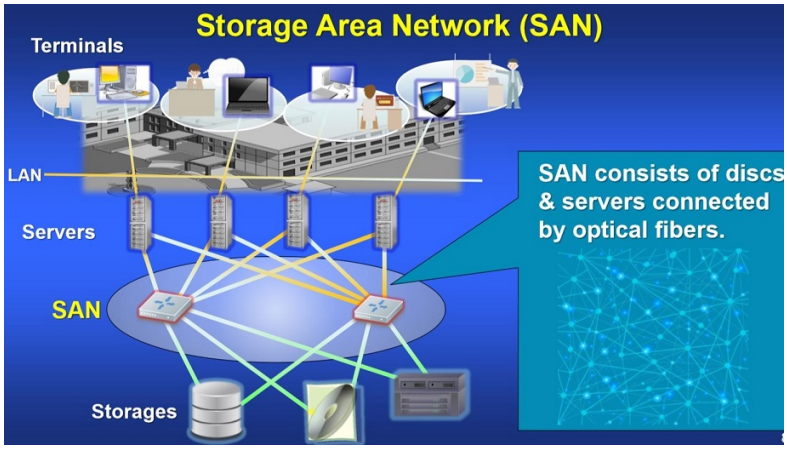

Figure 2.19. Storage area networks are also a possible use for secure QKD communications

Japan Free Space QKD

NICT is leading free space QKD in an 8-km test-bed in Tokyo with laser communication through the air (Figure 2.20).

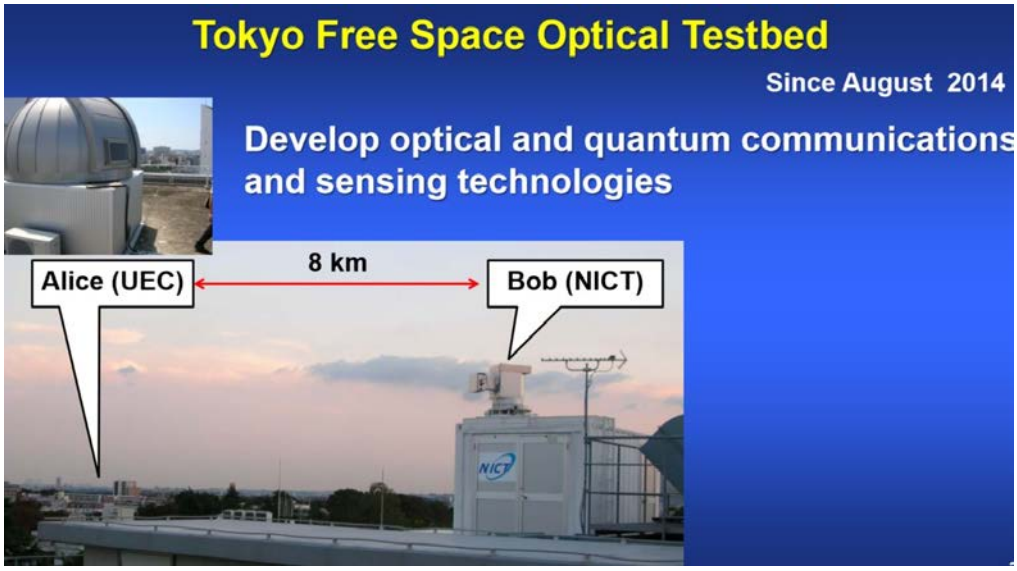

Figure 2.20. The 8km free space QKD network in Tokyo

Japan Satellite QKD:

Japan has ground-to-satellite laser quantum communications testing with their SOCRATES satellite (Figure 2.21). Another satellite is planned for 2016, and around 2019 Japan is planning a national relay network, as shown in Figure 2.22. Japan also plans to collaborate internationally (Figure 2.23).

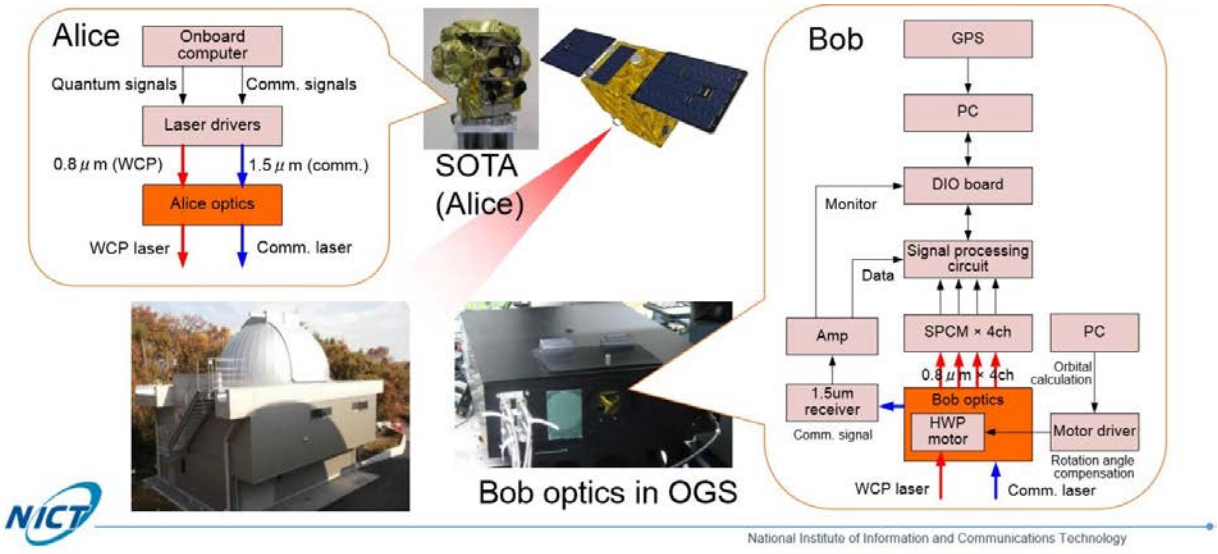

Figure 2.21. Japans' SOCRATES satellite and setup for QKD experiments

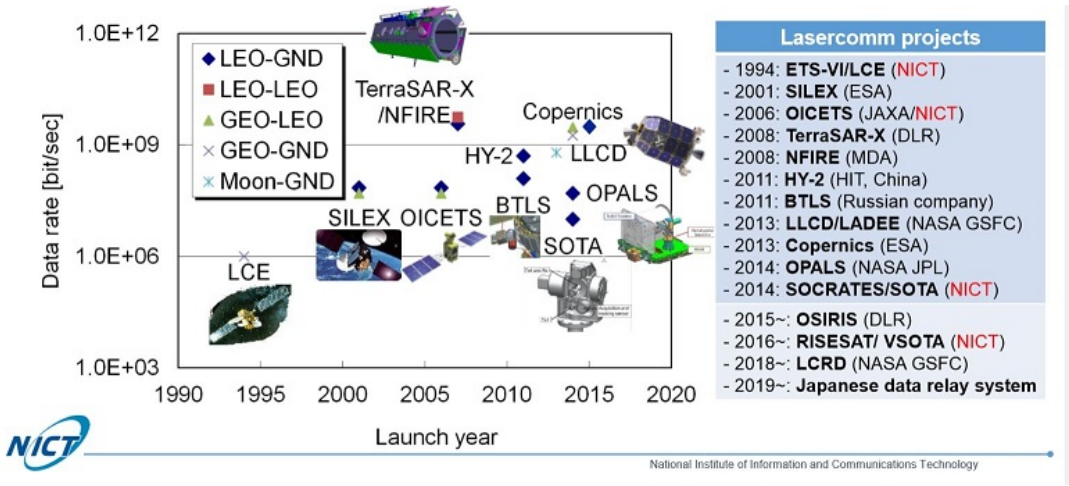

Figure 2.22. Timeline of satellites for laser communications

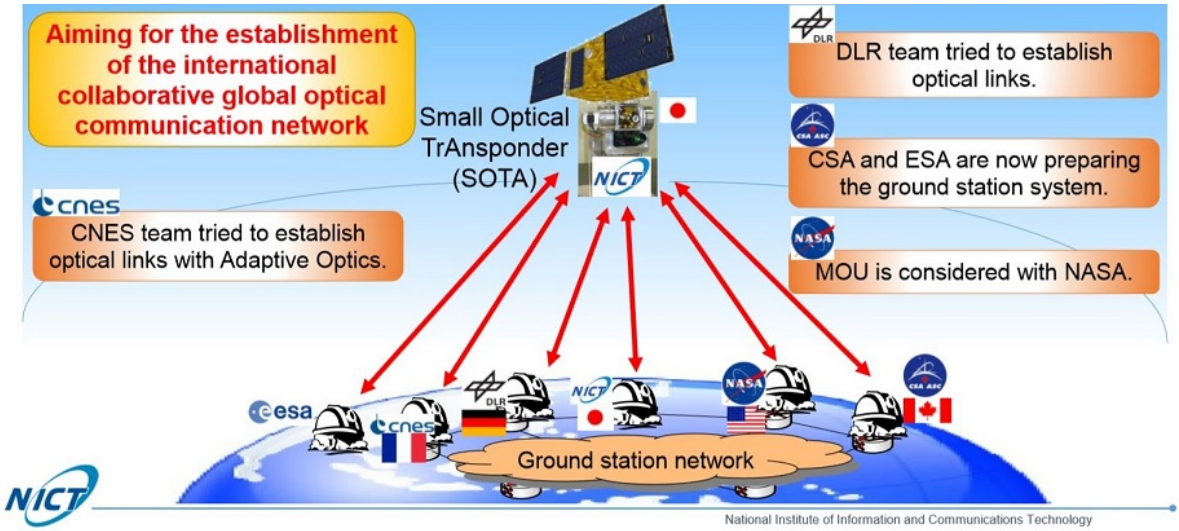

Figure 2.23. Japan plans international collaboration for space quantum communications

2.3.2 China QKD Network Developments

Optical Fiber QKD:

The University of Science and Technology of China (USTC) in Heifei is a leader in China in quantum communications and technologies, with research being led by Prof. Jian Wei PAN. His group is also leading in the development of QKD networks and their components. In some cases, the group is up to their fourth generation of QKD equipment. For recent developments, they invited companies such as ID Quantique, Qasky, Roi Optoelectronics and QuantumCtek to bid for the supply of QKD equipment, but it appears that ID Quantique did not place a bid, and QuantumCtek got the deal. PAN's team is presently in Phase 2 as described below:

Phase I: Approval test of quantum components

Phase 2: Indoor system debugging

Phase 3: Deployment

China's existing QKD networks are:

1. **The Heifei Intracity Quantum network**, which has 46 nodes (see Figure 2.24)

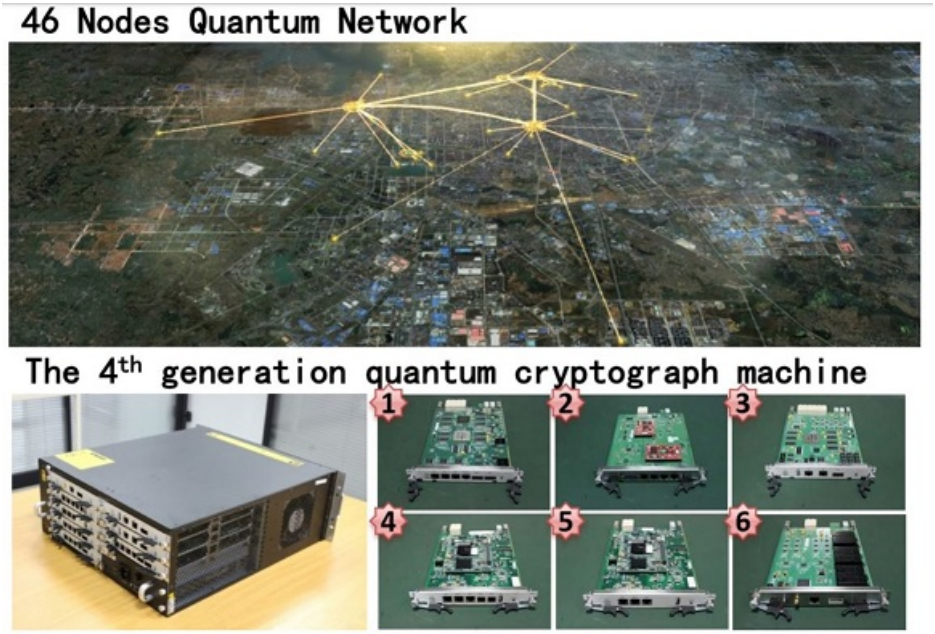

Figure 2.24. Heifei Intracity Quantum network

2. **Jinan Quantum Communications Network**, which has 50 nodes, 28 institutions, and 90 users over a 70-km^2 area, as shown in Figure 2.25 below.

Figure 2.25. Jinan quantum communications network

3. Plans for a 2000-km "Quantum Backbone" Network

A 2000-km QKD network is being planned to run between Beijing and Shanghai via Heifei and Jinan, as shown in Figure 2.26. This network will require quantum repeaters, but networks will be prepared in the four cities first.

Figure 2.26. Planned "quantum backbone" QKD network between Beijing and Shanghai

4. China Satellite QKD:

China's quantum science satellite will be launched around 2016, led by Prof. Jian-Weui PAN of USTC and in collaboration with European Space Agency and the University of Vienna (Figure 2.27).

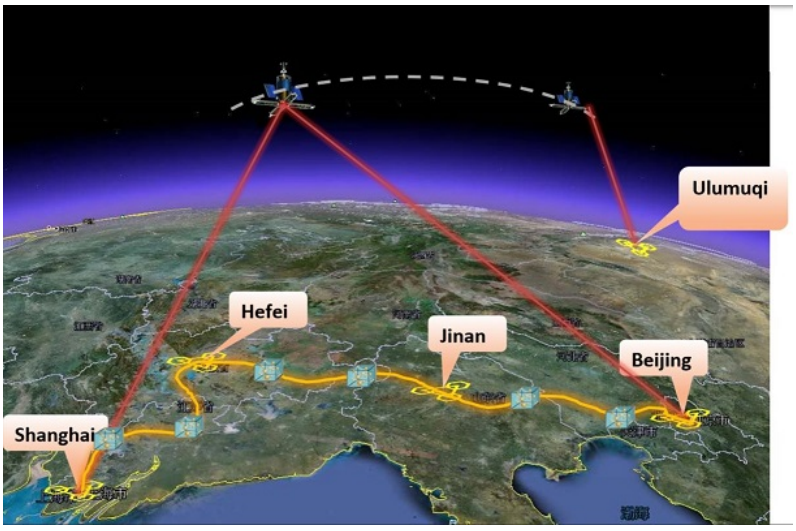

Figure 2.27. Image of China's planned satellite and land quantum communications networks

2.3.3 Vienna QKD Network Developments

Optical Fiber QKD Network

SECOQC QKD network in Vienna between institutions.

Free Space QKD:

Various developments led by Rupert URSIN of The Vienna University of Technology.

- Demonstrated QKD over 144km in Canary Islands (Figure 2.28).
- Also a 3-km test-bed in Vienna.

Satellite QKD:

Collaborating with USTC in China, as mentioned above in preceding section.

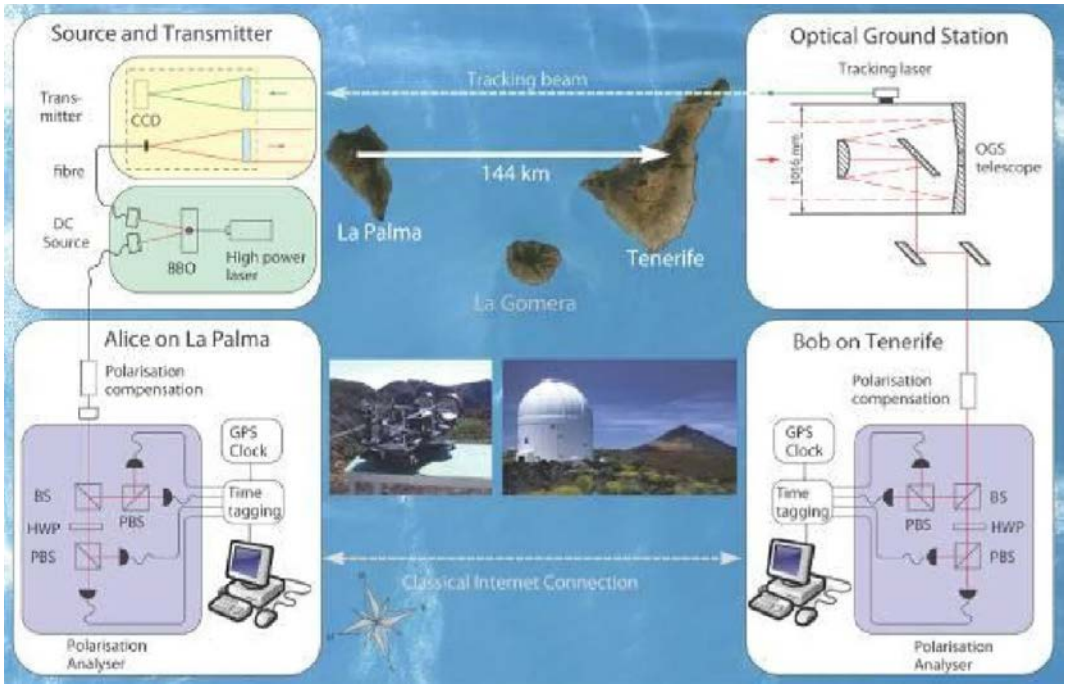

Figure 2.28. Demonstrated free space QKD over 144km in Canary Islands

2.3.4 Italy QKD Network Developments

- **Satellite QKD**

  Researchers at the University of Padova demonstrated quantum communication from a satellite in 2014, while in 2015 they have done single photon exchange to an MEO satellite as well as quantum interference by time-bin from an LEO satellite. They demonstrated that using polarization is also viable.

2.3.5 US QKD Network Developments

The US was a leader in QKD networks with the DARPA quantum network 15 years ago. A QKD network of the research organization Battelle was described at QCrypt 2015 (Figure

2.29). The QKD test-bed network has loops (4x110km, 8x25km) in Columbus, Ohio providing >400 km network (Figure 2.29). They are using ID Quantique QKD equipment.

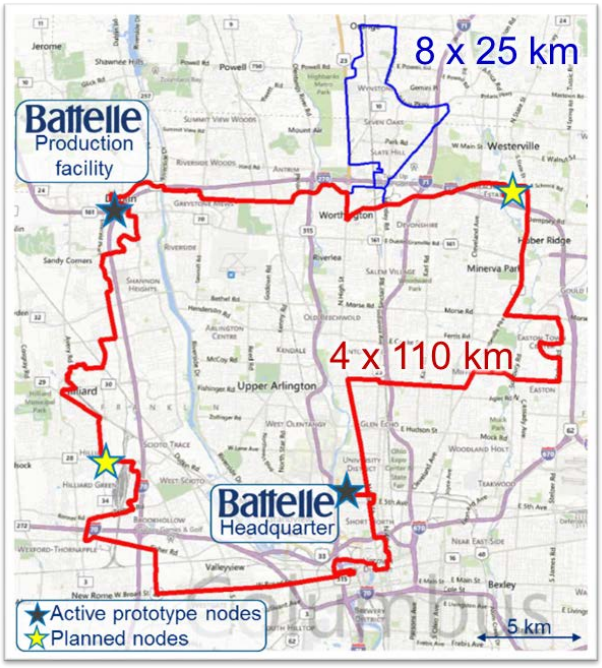

Figure 2.29. QKD network developed by Battelle in Columbus, Ohio (US)

2.4 QKD Component Developments

In order to improve the performance, robustness, and practicality of QKD systems there is continued development of next-generation equipment and methods. Some are described below.

- NEC has QKD equipment being trialed in the Tokyo QKD network, shown in Figure 2.30 below, which can provide a secure key rate faster than 1 Mbps. NEC is also trialing a hybrid QKD AES system as shown in Figure 2.31, where secure keys are transmitted via a QKD network.

Figure 2.30. NEC QKD equipment in the Tokyo QKD Network

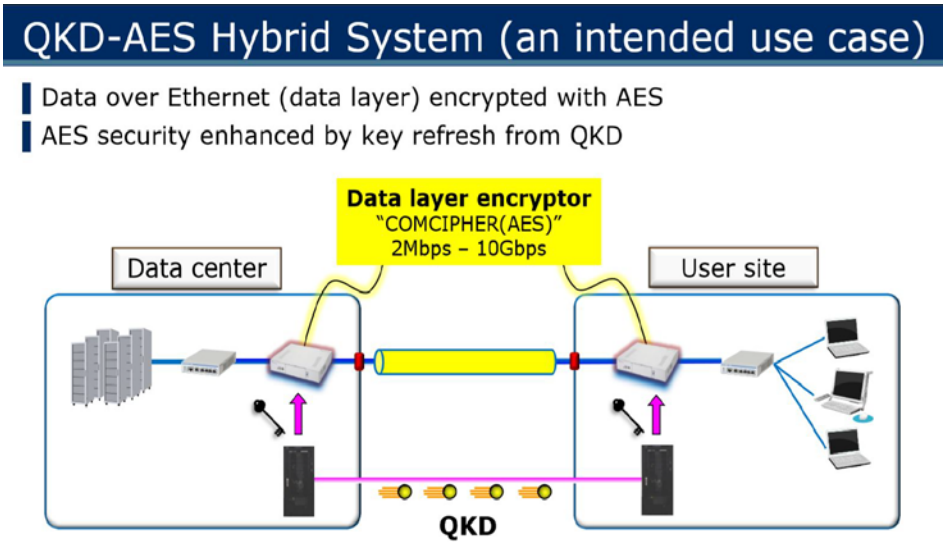

Figure 2.31. NEC's hybrid QKD-QES scheme where secure keys are transmitted via QKD network

- Toshiba was showing their third-generation QKD equipment (see Figure 2.32), with a secure key rate exceeding 1Mbps. They are not selling it yet.

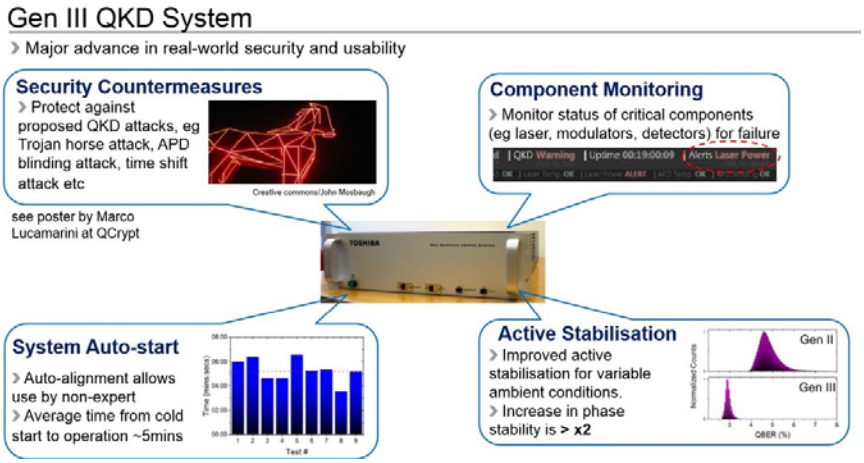

Figure 2.32. Toshiba's third generation QKD equipment (above), and its characteristics (below)

Separately, most QKD networks currently under development around the world are focused on the backbone network between several nodes. Toshiba, with developments focused in Europe, has also demonstrated that QKD can be integrated into standard GPON access networks too, as the network fans out to many users (Figure 2.33).

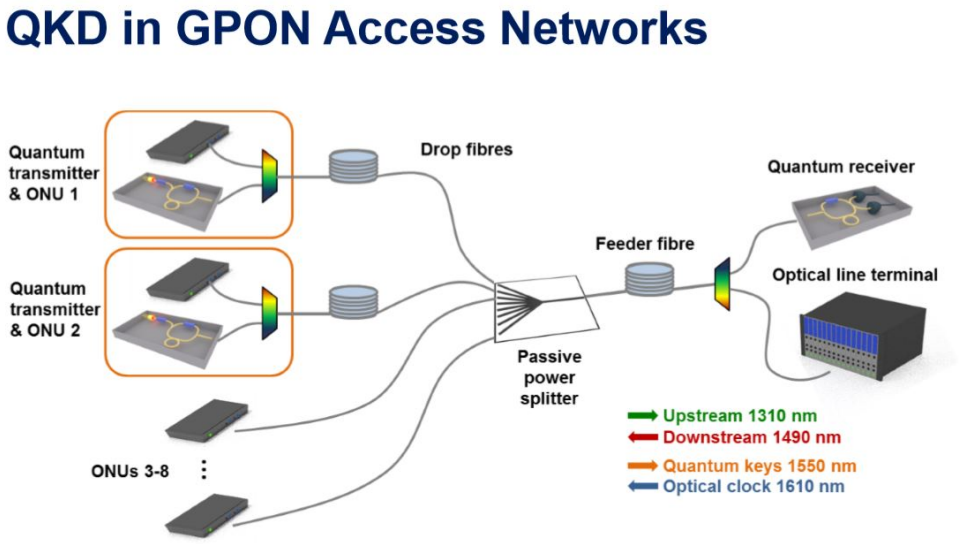

Figure 2.33. Toshiba has shown that QKD can also be used in access networks, not just backbone networks

- ID Quantique of Switzerland has been selling QKD systems since 2007, starting from their strength in random number generators. They say they have finally been getting business from company and bank users since 2014, trialing their systems (Figures 2.34 and 2.35).

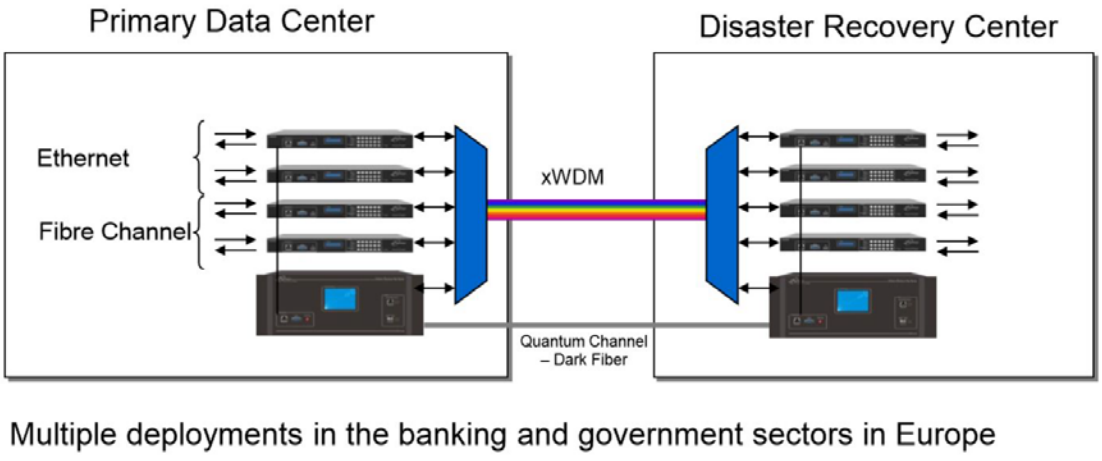

Figure 2.34. ID Quantique's example of QKD for data centers

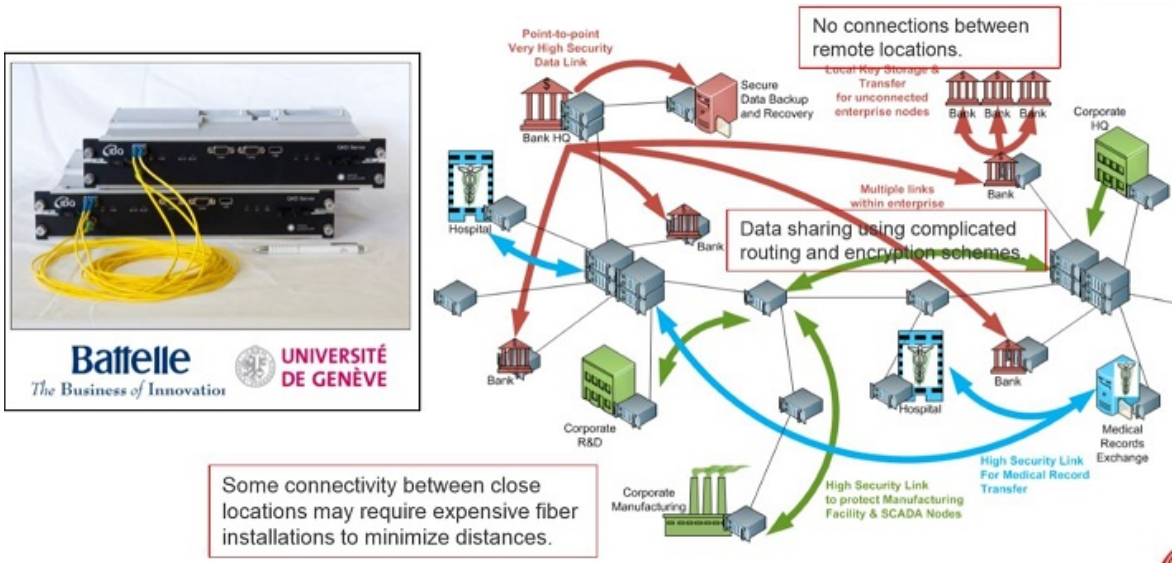

Figure 2.35. ID Quantique's image for moving toward quantum-safe communications

3. FURTHER RESEARCH HIGHLIGHTS

- **307-km QKD:** Hugo ZBINDEN et al. at The University of Geneva in Switzerland has demonstrated QKD over 307km with real-time secret key distillation. Distances greater than 300km approach the limit of QKD without quantum repeaters. This was achieved by having good components, such as using InGaAs avalanche photo diode detectors, and low-loss optical fibers (companies like Corning are working on even lower loss fibers). The researchers see a QKD engine producing 1Gbps of provably secret keys on the horizon.

- **Gbps secret key rates:** Jeffrey SHAPIRO et al. of MIT showed that using amplified spontaneous emission (ASE) and that homodyne detection is capable of 3.5-Gbps secret key rates over a distance of 50 km, which can defeat passive eavesdropping. To defeat active eavesdropping, ASE with homodyne detection is capable of 2 Gbps over 50 km.

  No new technology is needed to implement this ASE-homodyne protocol.

- **Improved speed of device-independent QKD:** Device-independent QKD has had very slow secure key rates. However, Andre SHIELDS et.al of Toshiba have achieved a 2 to 6 orders of magnitude improvement with key rates exceeding 1 Mbps over 10km or 100 kbps over 50km, which is only one order of magnitude less than QKD. This gives hope for the future of device-independent QKD. It took them two years, but the key was to use components better suited to device-independent QKD such as optically seeded pulsed laser sources to produce two indistinguishable sources.

- **Quantum photonic chips:** Many of the optical quantum entanglement experiments are done on optical benches measuring meters in length with thousands of components. Some groups around the world are shrinking that down to the centimeter scale by integrating the elements onto a chip (see Figure 3.1 below). Mark THOMPSON et al. from the University of Bristol (UK) described their pursuit of such.

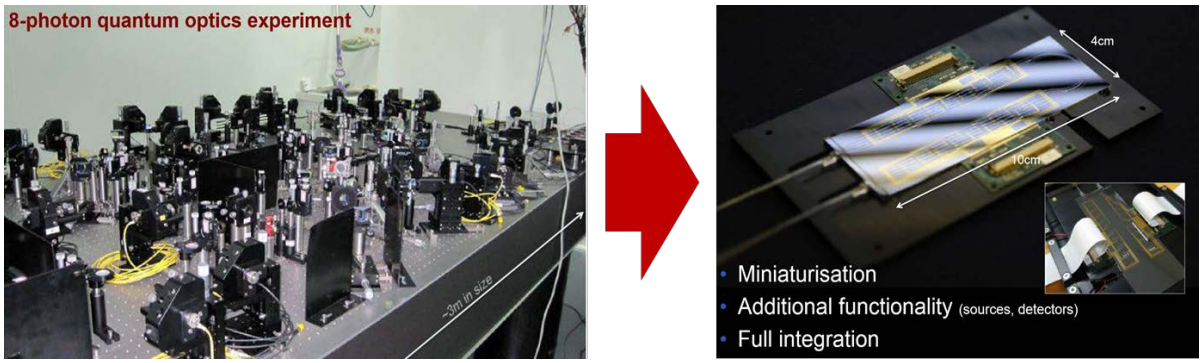

Figure 3.1. Quantum optics experiments on traditional optical bench (left), shrinking it down to chip size (right)

First, they have made micro-waveguides in glass using entanglement experiments with up to 6 photon sources - still not yet as many as on optical benches. A key feature is not just miniaturization, but also stability, since temperature can be controlled on-chip (Figure 3.2).

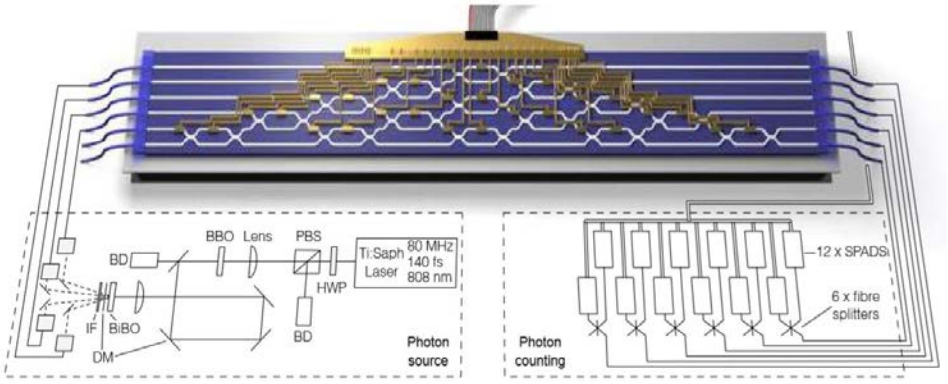

Figure 3.2. Image of optical waveguides integrated on glass chip

The researchers have also been making waveguides in silicon (Si), which further shrinks waveguide widths from microns to 450 nm in width. Not only that, but Si brings with it the standard semiconductor processes and equipment that can enable continued shrinking and integration, i.e., like a Moore's Law for photonic chips. Photon sources and detectors could also be integrated on-chip (Figure 3.3).

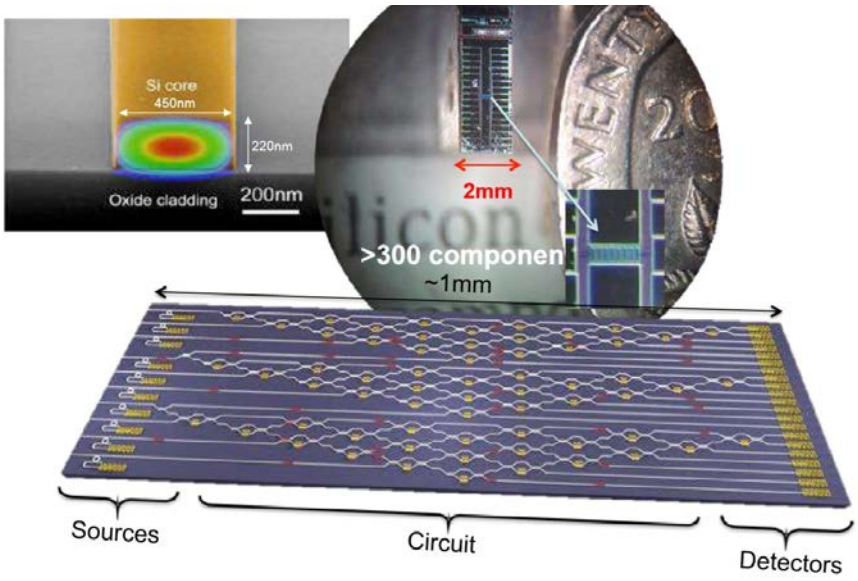

Figure 3.3. Images of photonic chip with optical waveguides for quantum entanglement experiments

THOMPSON et al. have shown Si photonic chips with five photon sources for entanglement and 100 components integrated on-chip. Classical optical chips have been made by others with 12,000 components integrated, demonstrating the integration possibilities for quantum chips. THOMPSON's group is presently working on various components such as photon sources and detectors. They have shown that QKD on-chip can provide a secret key rate up to 2.35Mbps over 20km, opening possibilities for shrinking the size of QKD equipment (Figure 3.4).

The researchers say that they may be able to get to eight-photon source systems in two years. For photon entanglement systems on standard optical-bench systems, some people see a limit up around 12 photons. However, doing it on-chip can solve some of the sources for such limits, so they think it is scalable beyond 12 photons.

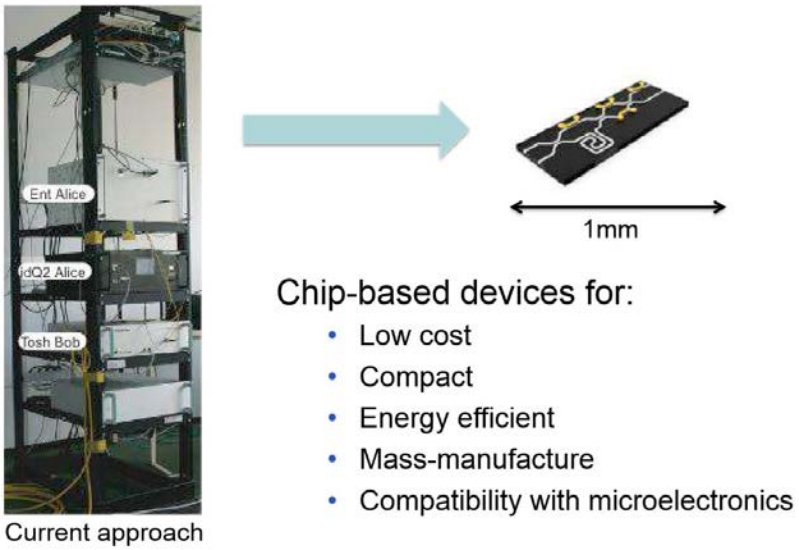

Figure 3.4. Image showing the advantages of shifting to QKD on-chip

- **First loophole-free violation of Bell inequality:** In a recent result that has become a focus of attention around the world, R. HANSON et al. of TU Delft in the Netherlands experimentally demonstrated the first loophole-free violation of Bell inequality. This demonstrated what Einstein called the "spookiness" of action-at-a-distance in the quantum realm. They entangled electron spins over a 1.3-km optical path that showed action at a distance by violating the Bell inequality.
- **All-photonic quantum repeaters without quantum memories proposal:** Koji AZUMA et al. of NTT in Japan have overturned conventional wisdom by proposing an all-photonic quantum repeater scheme that does not require quantum memories. Up until now, it was thought that quantum matter memories were required for the repeaters, which are a difficult issue to realize.

  Their scheme would solve the memory problem and could also operate at room temperature. The same principle can be used for optical-based quantum computers, and the protocol is easier than previously proposed schemes for such optical quantum computers.

  This new scheme has not been physically implemented yet, but the repeater is based on already-developed optical elements. Even so, it still may take 10-20 years to be implemented fully.

4. CONCLUSIONS

A big shift in perspective within the past year has resulted from the US NSA's announcement of plans for transitioning to quantum resistant algorithms. Since others will follow, there will be increased pressure to consider quantum risk. This may be the start of the "quantum era."

It is likely to be many years (maybe 10-20) before robust, large, and usable quantum computers are available, if at all feasible. However, it will also take time to prepare for such a world where we need "quantum-safe" systems that will be secure even if quantum computers are available to break existing cryptography such as RSA.

Post-quantum cryptography is showing some promise, and is more similar to traditional cryptography, while QKD provides ultimate security but needs new infrastructure. It is still too early to say, but both QKD and post-quantum cryptography may find areas of use. However, with legacy IT systems vendors not showing an interest in quantum technologies and traditional cryptography people not interested and limited in their understanding, what will they do when the time to become "quantum-safe" is an urgent necessity? From ATIP's perspective, if post-quantum cryptography shows real viability, then that may be the easier leap for the legacy people and organizations.

5. APPENDICES

5.1 Appendix A – Conference program, Abstracts, Poster List

There was no official proceedings book for this conference. The conference program, abstracts and a list of posters accompanies this report as a separate PDF file.

5.2 Appendix B – QCrypt & UQCC Conference Presentation Slides and Posters

Copies of the presentation slides and posters will be provided separately on USB.

5.3 Appendix C – Partial Participant List

There were 334 participants overall, including UQCC, and 277 attendees from 24 countries for QCrypt. A partial list of participants is provided below:

Speakers:

Johannes A. Buchmann (Technical University of Darmstadt)

Iordanis Kerenidis (Universite Paris Diderot, CNRS)

Hugues De Riedmatten (ICFO, Spain)

Akihisa Tomita (Hokkaido University)

Nicolas Gisin (University of Geneva)

Erika Andersson (Heriot-Watt University)

Liang Jiang (Yale University)

Carl A. Miller (University of Michigan)

Michele Mosca (IQC, University of Waterloo)

Graeme Smith (IBM Research)

Mark Thomson (University of Bristol)

Rupert Ursin (IQOQI, University of Vienna)

Hugo Zbinden (University of Geneva)

Boris Korzh (University of Geneva)

Yoshihisa Yamamoto (NII, Japan)

Artur Ekert (University of Oxford/Singapore National University)

Kae Nemoto (National Institute of Informatics, Japan)

Charles H. Bennett (IBM Research)

Gilles Brassard (Universite de Montreal)

Andrew Shields (Toshiba Research Europe)

Masahide Sasaki (NICT, Japan)

Ei Shimamura (NEC)
Nino Walenta (Battelle, US)
Bernd Fröhlich (Toshiba Europe)
Koji Azuma (NTT, Japan)
Patrick Cole (University of Waterloo)
David Elkouss (TU Delft)
Bill Munro (NTT, Japan)
Kai-Min Chung (Academia Sinica, Taiwan)
Stacey Jeffery (Caltech)
Dominique Unruh (University of Tartu, Estonia)
Hua Chen (USTC, China)
Poompong Chaiwongkhot (University of Waterloo, Canada)
Vladyslav Usenko (Palacky University, Czech Republic)
Christiana Varnava (Toshiba Research Europe, Cambridge University)
Hari Krovi (Raytheon BBN)
Robert Collins (Heriot-Watt University, Edinburgh)
Juan Miguel Arrazola (University of Waterloo)
Feihu Xu (University of Toronto)
Fabian Furrer (NTT, Japan)
Mario Berta (Caltech)
Alexandru Gheorghiu (University of Edinburgh)
Max Fillinger (CWI, Amsterdam)
Serge Fehr (CWI, Amsterdam)
Nicolas Brunner (Universite de Geneve)
Karol Horodecki (University of Gdansk, Poland)
Romain Alleaume (Telecom ParisTech)

Poster Presenters:

USTC, China
Hokkaido University
University of Oxford
Air Force Engineering University, China
Osaka University
MIT

Yokohama National University

Caltech

TU Delft

NUS, Singapore

Max Planck Institute

Universidad Politecnica de Madrid, Spain

Nihon University, Japan

NTT, Japan

NII, Japan

University of Calgary

NICT, Japan

Beijing University of Posts and Communications

Toshiba Research Europe

Heriot Watt University

University of Waterloo

Korea University

Peking University

Telecom ParisTech

University Paris Saclay, CNRS, France

Gakushuin University, Japan

Australian National University

Tokyo Institute of Technology

Austrian Institute of Technology

US Air Force, Institute of Technology

Louisiana State University

US Department of Defense

Some of the other Academic Participants:

University of Sydney
NIST
ETSI

University of Ottawa
University of Technology, Sydney
University of Copenhagen
KAIST (Korea)

University of Chicago
ETRI (Korea)
University of Texas, Austin
RIKEN (Japan)
Waseda University (Japan)

University of Electro-Communications (Japan)

Universidad Autonoma De Madrid (Spain)
University of Munich

Tel Aviv University
Yale University

University of York

Sophia University (Japan)

Some of the Corporate Participants:

Huawei Technologies, Research (Europe)
SK Telecom
ID Quantique (Switzerland) (had exhibit)
NTT (Japan)

Toshiba (had exhibit)
NEC (had exhibit)

Fujitsu

Mitsubishi Electric Corporation

Sumitomo Heavy Industries

IBM Research
Raytheon BBN

Whitewood (US) (had exhibit)

Quantum Opus (had exhibit)
Princeton Lightwave (had exhibit)

Japan Laser Corporation (had exhibit)

Low Noise Factory (had exhibit)

END OF REPORT

ATIP offers a full range of information services, including reports, assessments, briefings, visits, sample procurements, workshops, cultural/business sensitivity training, and liaison activities, all performed by our on-the-ground multilingual experts.

Email: info@atip.org Website: http://www.atip.org

Japan Office:
ATIP Japan
MBE 98
Yurakucho Building B1F
1-10-1 Yurakucho
Chiyoda-ku, Tokyo 100-0006

Tel: + 81 (90) 8858-6670

U.S. Office (HQ):
ATIP
PO Box 4510
Albuquerque, NM
87196-4510
USA

Tel: +1 (505) 842-9020
Fax: +1 (505) 766-5166

China Office:
ATIP
QingYun Modern Plaza, #2029
No. 43, W. Northern 3rd Ring Road
Haidian District
Beijing 100086 China

Tel: +86 (10) 6213-6752
Fax: +86 (10) 6213-6732

atip
asian technology information program