On Security Issues of QKD

This document is devoted mainly to solve confusions and doubts about the security of Quantum Key Distribution (QKD), and we also give some case studies where the use of QKD deserves to be considered.

Excerpt from a recent conversation between Alice, Bob and Eve

Alice: You know what Bob, I saw on TV that absolutely secure cryptography has come into play. It says “quantum something….”

Bob: Oh yeah, you mean quantum cryptography. But a recent newspaper article said something different.

Eve: Yeah, it was broken.

Alice: Really? Which one is true?

Bob: Look, I have also found something on the Web. What’s this?

Alice: Wow, here is also a document on practical security.

Eve: Probably another desperate effort to claim that QKD is absolutely secure.
I am already late for a meeting and should go!

Bob: No, wait, this summary looks quite different and interesting. It says …

What does this document explain and address?

1, Quick introduction of QKD and this document (page 4-9).

2, Can QKD work all by itself? (page 10)

3, What is a QKD protocol? What do we mean by “unconditionally secure”? (page 11-13)

4, What is a QKD implementation? Is it different from a QKD protocol? (page14 and page 15)

5, What is a side channel? Does it exist only in QKD? What kinds of side-channels exist? (page15-18)

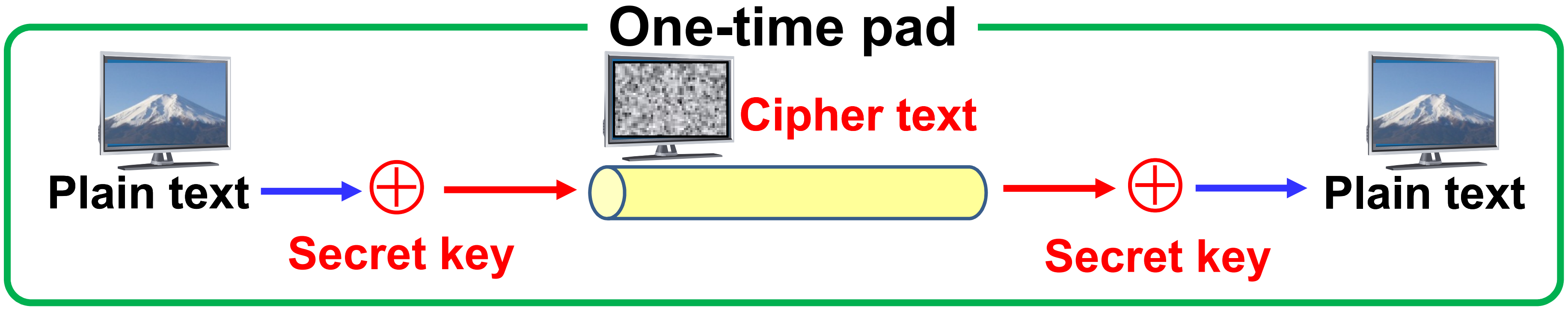
6, Answers to some criticisms or questions from non-quantum crypto communities, and open questions (page 19-22).

7, On some potential applications of QKD (page 23).

8, We have some appendices for further readings (from page 24).

One-time pad

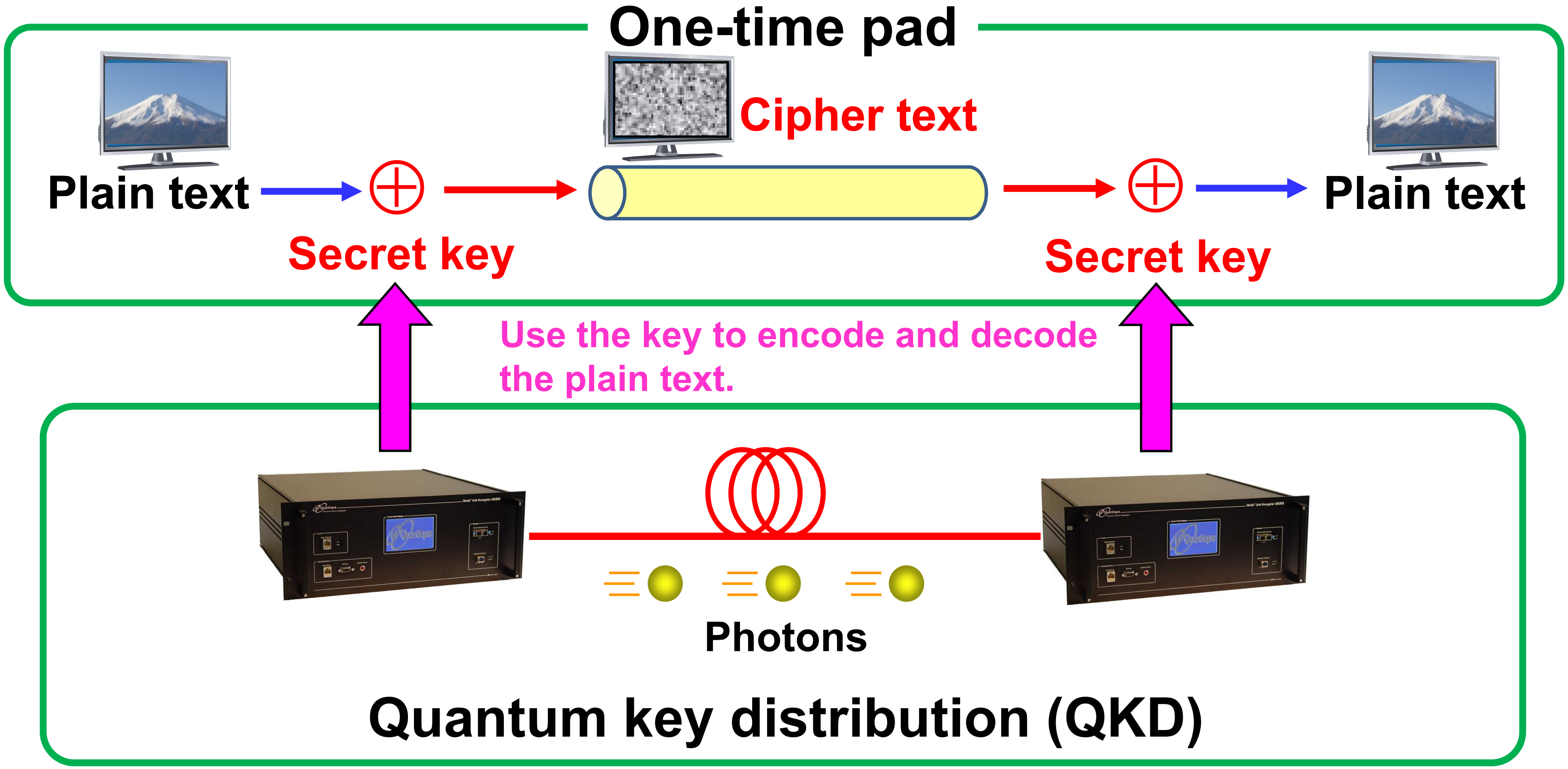
Among all the methods of encryption ever devised, only one has been proven to be information-theoretically secure, i.e. secure against an eavesdropper who has unbounded ability, often also referred to as unconditionally secure.
It is the one-time pad (OTP). The key should be used only once and be as long as the message to be sent. The efficient distribution of such long keys remains an issue.



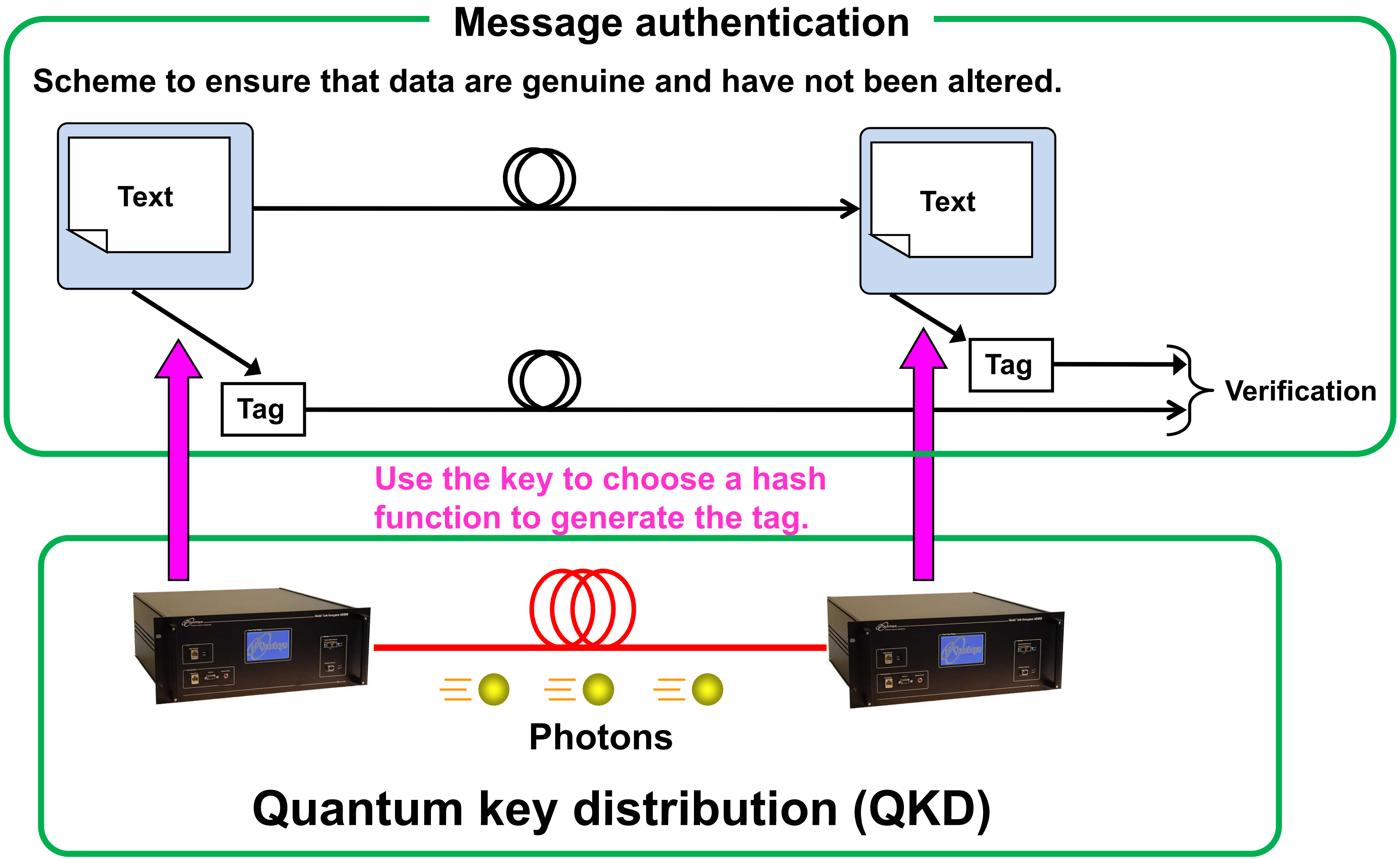
So far trusted courier is only the method of delivering secret key.

QKD offers the function of key exchange

Quantum key distribution (QKD) provides a means to distribute unconditionally secure key for OTP, using photons over an optical network. Key exchange (or key distribution) is at the heart of cryptography. Secure key by QKD can be used for many applications including secure communications and message authentication (MA) over any standard communication channels.


One-time pad
Cipher text
Plain text
⊕
Secret key
⊕
Plain text
Secret key
Use the key to encode and decode the plain text.
Photons
Quantum key distribution (QKD)

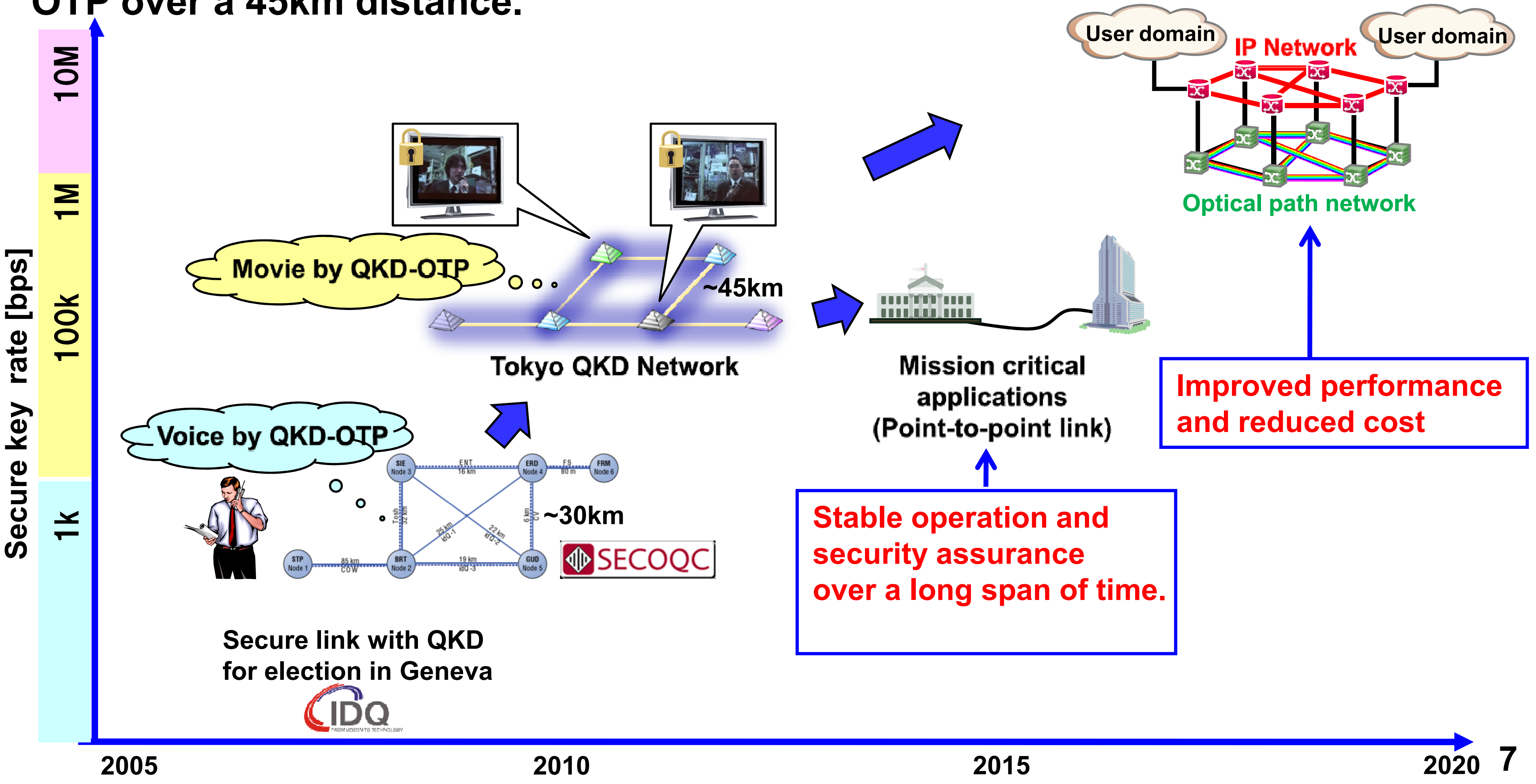
QKD offers the function of key exchange


Message authentication
Scheme to ensure that data are genuine and have not been altered.
Text
Text
Tag
Tag
Verification
Use the key to choose a hash function to generate the tag.
Photons
Quantum key distribution (QKD)

QKD can be used for any application that requires the key!

Towards a wider acceptance of QKD

For the past ten years, QKD research has been engaged in field network demonstration. In 2007, ID Quantique made the first use case of QKD for the election in Geneva. In 2008, the EU project, SECOQC, demonstrated a QKD network, which could encrypt voice transmission by OTP over a 30km distance. In 2010, the Tokyo QKD network demonstrated secure TV conferencing with OTP over a 45km distance.



Secure link with QKD for election in Geneva

Tokyo QKD Network

Mission critical applications (Point-to-point link)

Stable operation and security assurance over a long span of time.

Improved performance and reduced cost

Thus QKD technology edges ever-closer to practical use. The near-term use case is likely to be high-end security applications that have been relying up to now on trusted couriers for key exchange. To become a practical solution, long-term reliability of QKD needs to be guaranteed. This includes not only stable operation but also security assurance over a long span of time. The latter is especially a non-trivial and much involved issue, and hence is a motivation of this document.

Implementation of QKD in a closer form of ideal theory is not an easy task at all. It still comes at a price. But once realized with cheaper cost in the future, QKD technology would have a big impact on key exchange infrastructure, enhancing the security significantly. QKD technology will then be installed into IP over optical network infrastructure. One could download an ultimately secure key to use it in many applications, including OTP and message authentication (MA), with high security. Encryption and decryption in OTP and MA are quite simple, just addition of the key to a plain text. Hence no latency occurs. It would get rid of our reluctance to introduce cryptography in daily life, which often causes inconvenience in our PC, slowing down the processing speed.

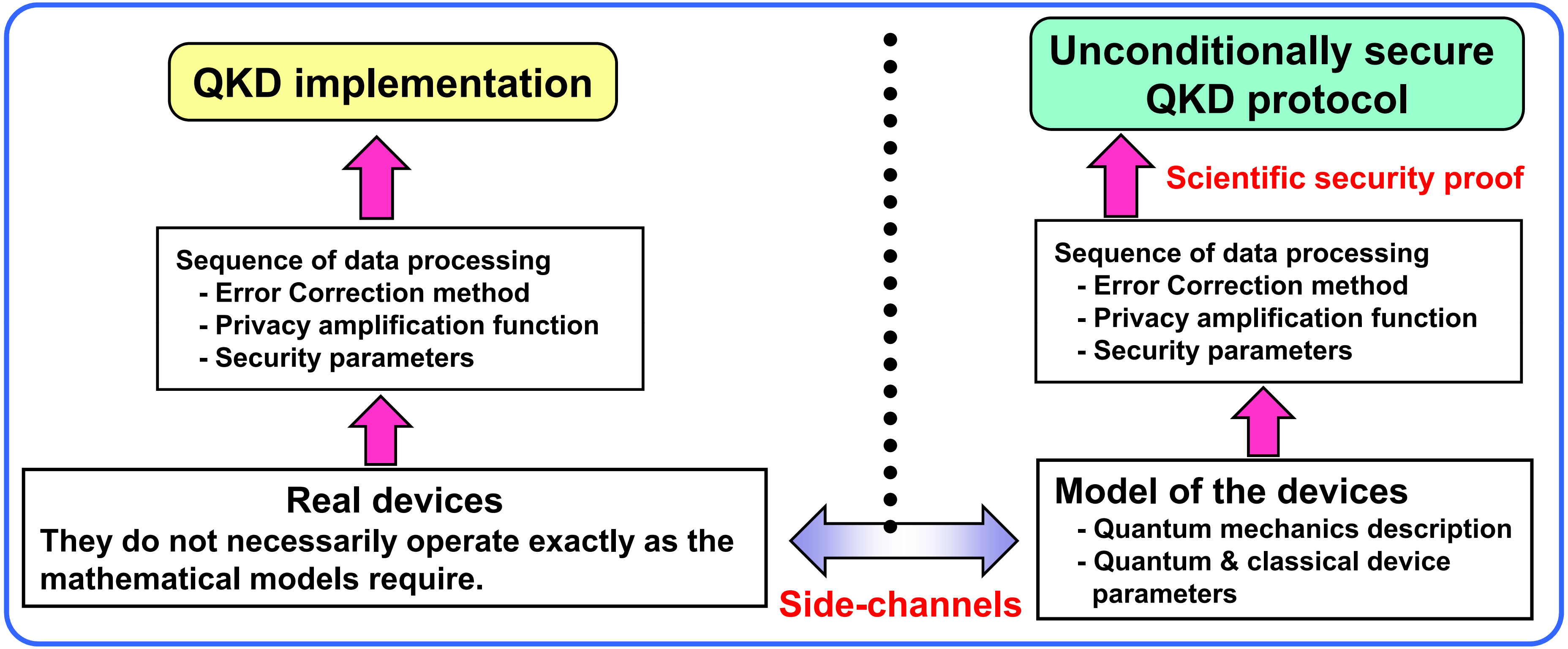
This may be the major impetus to pursue the improvement of QKD technology and future QKD network research. However, we should first clarify the issue of security assurance of practical QKD systems in which imperfections are inevitable to some extent .

The main issues in this document

A catchy statement that QKD can ensure the unconditional security often causes confusion, and even doubt sometimes. In this document, we would like to explain the difference between QKD *protocol* and its *implementation*, addressing issues on side-channels, and give a clear perspective of QKD.

We also discuss an issue of QKD versus key delivery by courier.

(1) QKD protocol and its implementation



QKD implementation

Sequence of data processing
- Error Correction method
- Privacy amplification function
- Security parameters

Real devices
They do not necessarily operate exactly as the mathematical models require.

Side-channels

Unconditionally secure QKD protocol

Scientific security proof

Sequence of data processing
- Error Correction method
- Privacy amplification function
- Security parameters

Model of the devices
- Quantum mechanics description
- Quantum & classical device parameters

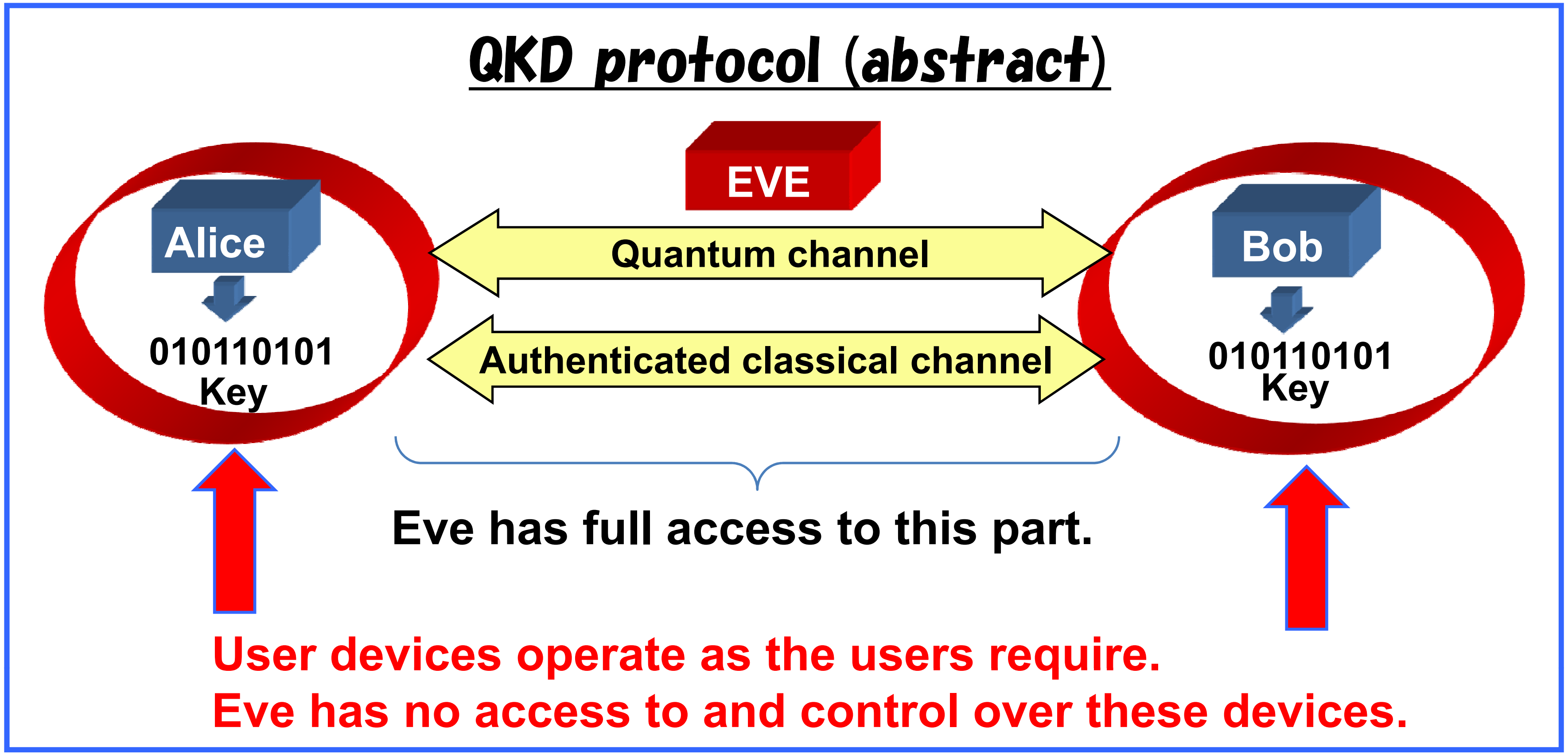
(2) Discussion on key distribution by a courier

Can QKD work all by itself?

A QKD protocol cannot work only by itself, and it needs to authenticate the classical messages that are exchanged between Alice and Bob. Typically, we use the Wegman-Carter type authentication protocol, which is unconditionally secure at the expense of consuming a small portion of the key.

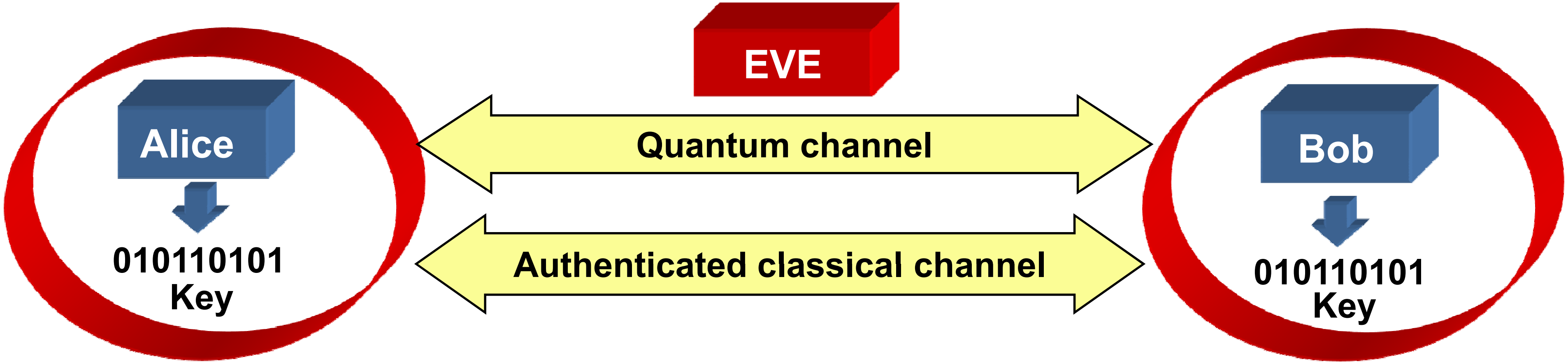
The use of the Wegman-Carter type authentication protocol requires the initial key for the very first run of a QKD protocol. Note that since this key is used only for the authentication, it needs to be secure only until the end of the authentication. For the next rounds of the QKD protocol, we can use the key generated in the previous rounds. Due to the consumption of the key, a QKD protocol is sometimes called a “key growing” or “key expansion protocol”.

Unconditional security of QKD protocol


QKD protocol (abstract)
EVE
Alice
010110101
Key
Quantum channel
Authenticated classical channel
Bob
010110101
Key
Eve has full access to this part.
User devices operate as the users require.
Eve has no access to and control over these devices.

- A QKD protocol is an abstract mathematical procedure.
- “Unconditional security” means “information theoretical security”. Namely, no conditions are set on computational power or resources available to Eve, but on the other hand we *do* need conditions on users’ devices, which have to operate as the users require and never allow Eve’s access.
- The key in future remains always as secure as at the time of creation (forward security).

Ingredients of a QKD protocol



A QKD protocol consists of the following two parts:

(I) Quantum communication (no need for authentication)

Alice and Bob communicate by quantum signals to achieve strong enough correlation for the key distillation.

(II) Post-processing (needs authentication): This communication is done over an authenticated classical channel. This communication includes:

(1) Sacrifice some data as test bits to estimate how much information/correlation about Alice and Bob's data Eve has.

(2) Error correction to agree on the key: The error correction protocol can be either one-way (e.g. LDPC) or two-way (e.g. Cascade code).

(3) Privacy amplification: distill the key from the correlation.

Security definition of a QKD protocol

The security criteria are chosen on the basis of the following conditions (composable security):

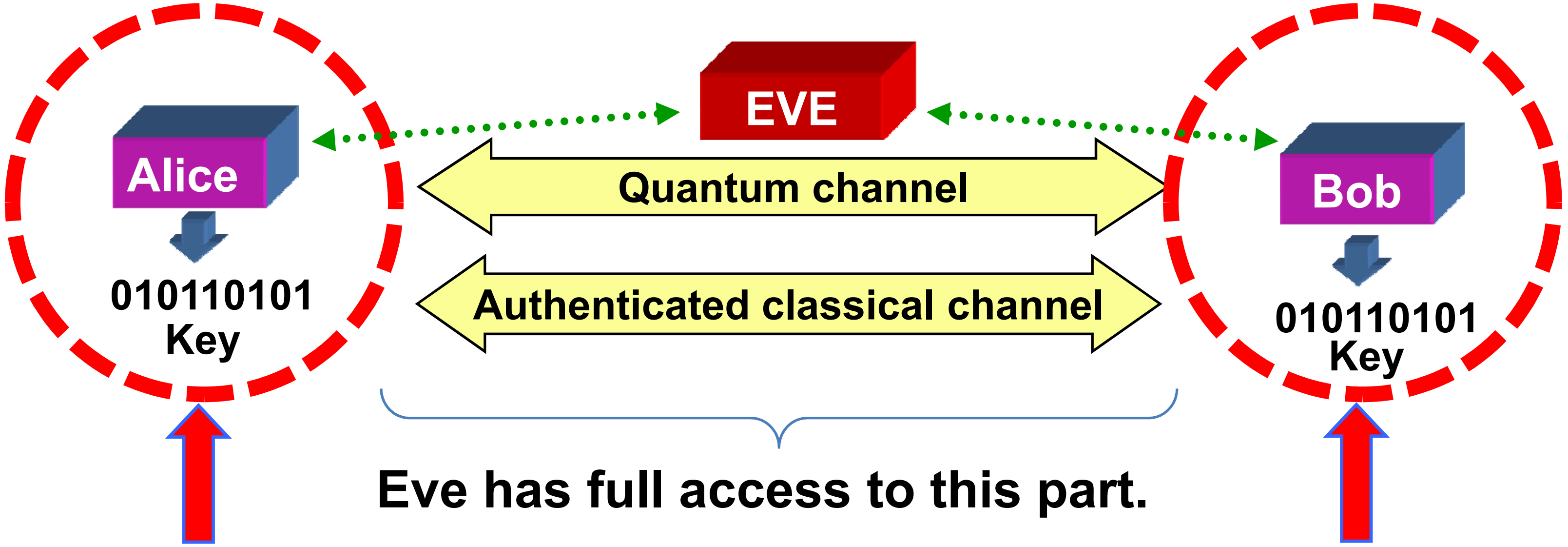
The imperfection should not increase even if the generated key is used for any applications in a larger cryptographic protocol, and the imperfection of the larger protocol is given by the summation of the imperfections of the component protocols.

It is known that this condition can be satisfied by the security definition being only with respect to the ideal situation, whose intuition is given below.

In terms of mathematics, this security definition asks how much an eavesdropper or a "distinguisher" can discriminate between the real situation and ideal situation. In the real situation, Eve or the distinguisher is in the possession of her own system, which may be correlated with the generated key, and moreover the generated key itself is given. On the other hand in the ideal situation, she is in the possession of the perfect key and some system independent of the perfect key. To measure the quality of the generated key, the maximum distinguishing probability is employed. See the appendix (page 25) for more explanation.
We emphasize that this distinguishing probability in terms of the ideal situation is the security measure we adopt, and we do *not* use any other information measures such as mutual information.

A QKD implementation

Implementation of a QKD protocol



Eve has full access to this part.

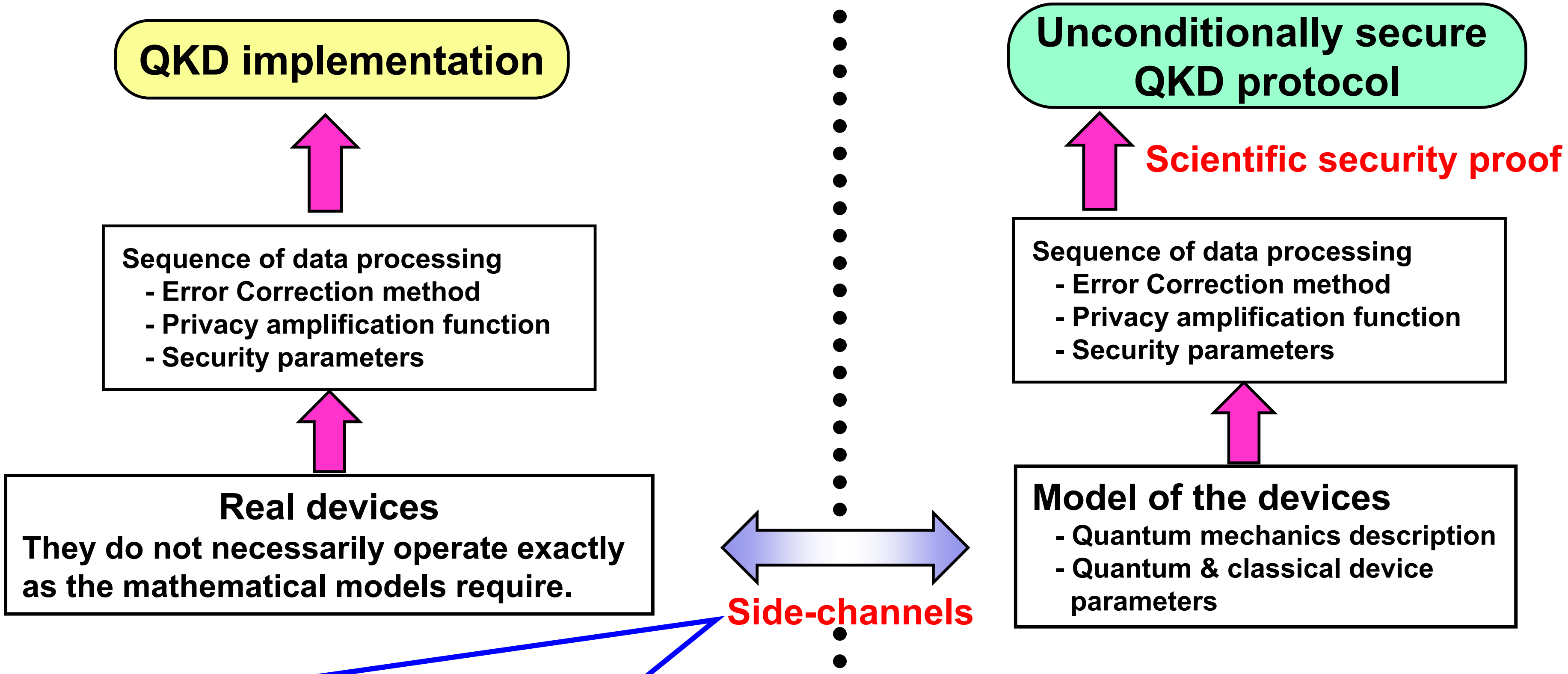
Eve has partial access to the devices, and they may not operate as the users require (these imperfection is called a side-channel).

- In a real implementation of a QKD protocol, Eve could have some access to the devices, or they could not operate as the users expect. These imperfections are called “side-channels”.

- Since the QKD protocol is unconditionally secure, we need to worry about only side-channels in the implementation. For all the modern cryptographic methods, both protocols and their implementations are in danger. This is an advantage of QKD over modern cryptographic methods.

On a QKD protocol and its implementation

- Based on the model of devices we can give a scientific (mathematical and physical) security proof of the QKD protocol, and in reality QKD implementation is based on real devices. *Like all security systems, how to confirm/achieve the model is a different story.*



QKD implementation

Sequence of data processing
- Error Correction method
- Privacy amplification function
- Security parameters

Real devices
They do not necessarily operate exactly as the mathematical models require.

Unconditionally secure QKD protocol

Scientific security proof

Sequence of data processing
- Error Correction method
- Privacy amplification function
- Security parameters

Model of the devices
- Quantum mechanics description
- Quantum & classical device parameters

Side-channels

A gap exists between the model of the devices for the security proof and its actual implementation.
It can be made small by technological development and theoretical advancement, but never vanishes.

- Since information is always carried, detected, and processed by a physical system, the same gap exists for all security systems, including modern cryptosystems.

On side channels of QKD implementations (1)

- Some side channels of QKD implementations are the same as those in non-quantum communications (Modern cryptography).

Side channels in common with standard communications.

Information leakage from classical data processors (for authentication, sampling, error correction, privacy amplification, key management, etc) and classical information storages due to unwanted emission of electromagnetic wave, which is the so-called tempest attack, and the leakage due to implementation errors (software bugs etc).

Examples of these side channels include emissions from devices, e.g. by means of electromagnetic, mechanical, and/or acoustical signals.

Side channels that may or may not be in common with standard communications

Response of the quantum devices to Eve's probe signals, e.g., the use of imperfect random number generators, etc.

For instance, Eve may shine a bright probe light into Alice's device through an optical fiber and monitor the reflective light to see which phase modulations Alice applies. See also Appendix for countermeasures.

On side channels of QKD implementations (2)

Purely quantum side channels

Side channel due to imperfections of devices which manipulate/detect quantum signals

Examples include mismatch in quantum efficiencies of the photon detectors and imperfect signal modulations, etc. Also see Appendix for the countermeasure.

- **Identifying side-channels and patching loopholes is vital for *any* cryptographic system, whether it is quantum or classical.**
- **We need to find a common level of acceptance of side-channels. Sharing information on side-channels gained from modern cryptography as well as from past, current and future QKD activities is the key to derive a common denominator for security certification standards.**
- **The quantum side-channels might be removed with the development of the theory (based on Bell inequality) and technologies. A precise description of the devices might not be needed to provide security.**

Updating security certification technology

- We have to continuously look for new side channels, implement countermeasures, and update security certification technology, via the following R&D cycle.

(1) Implement QKD system

(2) Propose Loophole/ Hacking Method

(3) Implement hacking

(4) Propose countermeasure

(5) Implement countermeasure

(6) Battle-testing countermeasure

(7) If the countermeasure works, go back to (2),
and if it does not, go back to (4).

In these years, QKD may be in research on steps between (2) and (5).
So proposing hacking is highly welcome.

Why don’t you ask a courier to distribute the key?

Some people claim that since QKD assumes a courier to securely distribute the key for the first run of the authentication in QKD anyway, why don’t we use the courier all the time? To address this issue, we list up some factors of the courier and the storage that the users use to store the key either from the courier or QKD.

Courier
- (C1) Can we use the courier more than once (availability)?
- (C2) Can we trust the courier (reliability)?

Storage of the key: (S) Is the storage perfectly protected from side-channels?

We emphasize that only if *all* the answers to the above questions are positive, then we can use the courier with the storage. In all the other cases, QKD deserves to the consideration to use as long as the communication distance is within its QKD reach. For instance…

(1) If the answer to (C1) is “No”, then QKD has an advantage over the courier since QKD offers a way to expand the key whenever needed. Note that this answer is “No” in the case, for instance in earth-satellite communications or whenever the courier’s availability is limited by the cost or by other practical factors.

Why don’t you ask a courier to distribute the key?

Courier
- **(C1) Can we use the courier more than once (availability)?**
- **(C2) Can we trust the courier (reliability)?**

Storage of the key: (S) Is the storage perfectly protected from side-channels?

(2) If the answer to (C2) is “No”, QKD can instead use modern crypto or other means for the very first round of authentication, which are likely to be secure only until the end of the first run of authentication. It follows that if a modern cryptography protocol can be proven to be secure for at least a small period of time, then QKD protocol that calls the protocol only for the very first run is unconditionally secure.

(3) Suppose that both the answers to (C1) and (S) are “No”. In this case, the courier have to bring a key being large enough for life-time use. Note that this is dangerous since if the degradation of the stored key occurs in time, then all the keys distributed by the courier are corrupted at some point. On the contrary, QKD can offer a means to provide fresh keys whenever needed. If the degradation speed is slower than the speed of key generation and we use the generated key before degradation, then QKD clearly has advantage over the courier.

After all, whether a QKD implementation or the unsophisticated key delivery via courier is better depends on the underlying assumptions and the related technologies.

Other questions on QKD

(Q1) In OTP, the quality of random numbers is important and it is extremely difficult to generate true random numbers. For instance, the guessing probability of all the bits of the perfect key is $2^{-10^5} \approx 10^{-30100}$ (here, 10^5 bits is an example of key length generated per second) and this probability is not achieved in all QKD systems.

(A1) In QKD, we do *not* demand the key to have all the qualities that the perfect key has, but instead we demand that the imperfections do not increase, as imposed by the security definition (see the slide entitled with "security definition of QKD protocol").

Roughly speaking, we allow the guessing probability of 10^{-6}, which is reasonable in reality, and more importantly, we can make this number smaller if we want. In other words, since 2^{-10^5} is a ridiculously small probability (comparable to a single disaster event in the whole life time of the universe) it would be meaningless to apply it in practice.

(Q2) QKD needs a lot of high quality random numbers, and how do we generate them?

(A2) It is true that, to date, one of the assumptions of the QKD theory is to have high-quality random numbers. However, it has not been demonstrated that without such numbers QKD becomes insecure. In other words, it may be possible that the assumption about truly random number can be removed without compromising the QKD security. Some researchers are investigating these issues. On the other hand, the development of the physical random number generators are also being undertaken to generate high quality randomness as fast as possible.

Other questions on QKD

(Q3) QKD basically works only on a point to point link, and it is not suitable for the internet.

(A3) QKD is not a universal tool, but QKD is suitable for some specific applications. We have to look for as much potential applications as possible, together with experts from the field of modern cryptography.

(Q4) Are there open questions, which can be addressed jointly by the QKD community and the Modern cryptography community?

(A4) Beside the issue mentioned in the previous point, another important issue is the one concerning side-channels, which affect all the communications, both classical and quantum.

Another interesting problem is how to combine QKD with existing modern cryptosystems to attain an improvement in the security of them. For instance, QKD could be used to refresh the keys employed in AES. We believe there are more works to be done together.

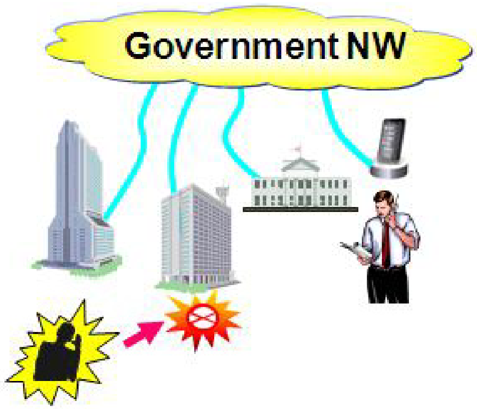
Potential applications of updated QKD

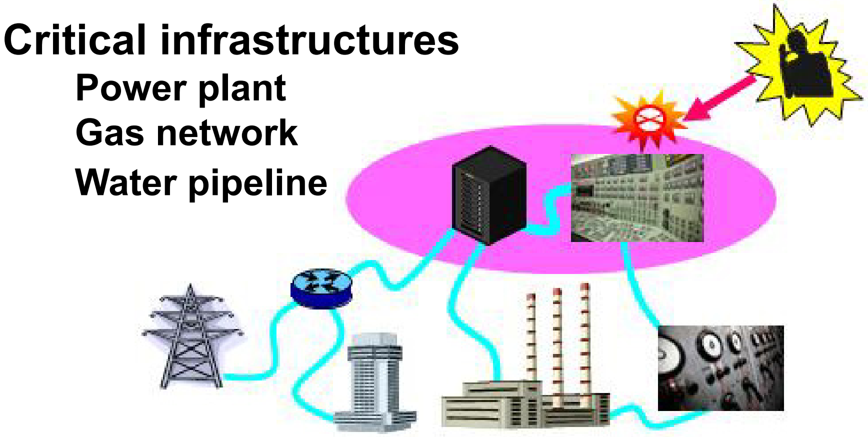
- Besides encryption of messages, application to key exchange for authentication and message integrity can be realized.

- The first target of QKD secure network will be government agency networks, for which state secrets need to be tightly protected at any cost.

- Applications will extend to the protection of mission critical infrastructures such as power plants and facilities for water and gas supply. In these facilities, surveillance and control data should be tightly protected by QKD secure network.

- QKD technologies are also expected to show their strengths in sensing small variations in the characteristics of optical fibers.




Critical infrastructures

Power plant

Gas network

Water pipeline

We remark that currently one needs to assume trusted node networks, which will be removed in future by introducing other quantum technologies.

A few days later Alice, Bob and Eve meet again…

Alice: OK, I got it. This document says that we have to be careful about the difference between a protocol and its implementation. The implementation always comes with side channels. But no one will ever be able to break a QKD protocol. Only its implementation may be broken by exploiting the side channels.

Bob: Yeah, some people mix this up, and that has made all of us very confused. I believe that if the QKD community continues to work hard on the identification of side channels in collaboration with modern crypto people and communication engineers, the side channel issue will be solved to a sufficient extent at some point in the near future.

Eve: Oh come on, there is always a little side channel that can be exploited, isn't it?

Alice: That is the case for any communication technologies and we need a cutoff at some point anyway. At least QKD has a big potential to realize very secure communication. But of course with some compromise in communication distances and speed.

Bob: Yes, but even if QKD becomes mature, we may still need modern crypto for many applications since the performance of QKD has some limitations as Alice mentioned. By the way, do you guys think that QKD can become practical for daily use?

Eve: Hackers won't be intimidated just because it says "quantum".

Alice: We'll see, but in the near future I believe QKD has a potential for special use cases as mentioned here. Anyway, QKD has a new functionality, and moreover it is still a growing area. So, it's too early to judge now whether QKD will have a broad application. Let's see what QKD will bring us in the future!

Postscript and acknowledgement

With the increase in the number of QKD network field tests (as well as the development of the related technologies and theory), QKD has attracted more interest not only from the quantum information society, but also from experts of other disciplines, including modern cryptography and the mass media. Feedbacks from non-experts of QKD are very important for the success of QKD as well as its long term adoption. Some of their arguments are critical, and some of them are actually relevant and deserve to be discussed.

The purposes of the UQCC2010 were to offer an opportunity for it, and also to show the status of the latest QKD technology. The UQCC2010 committees (an initiative by the Task Force) and the Tokyo QKD network project members took this opportunity, with valuable supports from many external experts, to present a document which gives non-experts a clear perspective of QKD, having the feedback (both positive and negative) we have received. We sincerely appreciate all the valuable supports and comments that the external experts have kindly made. More importantly, we sincerely acknowledge modern cryptographers, including Prof. Adi Shamir, who have made valuable criticisms. This gives the QKD community a chance to consider potential applications and ontology of QKD. It also stimulates valuable interdisciplinary discussions. We hope the QKD and non-quantum communities continue to collaborate to make cryptography society richer, both in terms of pure science and practical technology.

Acknowledgement

The UQCC2010 Task Force, Organizing Committees, and Tokyo QKD Network Project members express our sincere gratitude to :

N. Lütkenhaus, M. Koashi, M. Curty, H-K. Lo, B. Qi, L. Lydersen,
G. Kato, K. Azuma, M. Lucamarini, W. J. Munro, C-H. F. Fung, X. Ma,
M. Mosca, V. Makarov, P. Tombesi, T. Yamamoto, J. Skaar, N. Gisin

Some valuable slides in this document were provided by them.
They also have made significant efforts to improve this document.

UQCC2010 Task Force:

K. Tamaki (Chair), M. Peev, J. F. Dynes, M. Legré, A. Tajima, H. Takesue, T. Tsurumaru

Tokyo QKD Network Project:

M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev,and A. Zeilinger

UQCC2010 Organizing Committee:

K. Imafuku, M. Matsui, M. Sasaki(Chair), A. Shields, Y. Tokura, A. Tomita, A. Yamagishi

Appendix

Comment on the security definition of QKD (1)

Mathematically, we call the key is ε-secure if $||\rho_{SE} - \rho_U \otimes \rho_E||_1 \leq \epsilon$ holds, where ρ_{SE} is a joint quantum state of the real key and Eve's system after the eavesdropping, ρ_U denotes the perfect key, ρ_E is some state, and $|| \cdot ||_1$ represents the trace distance. In all the formal security proofs, this criteria is adopted, and the exponent of ε is called security parameter, which can be arbitrary fixed according to the user's demands.

The trace distance gives us an upper bound of the distinguishing probability (total variation distance), which is the probability of correctly discriminating the two situations (the ideal situation and the real situation) being maximized over all measurement that the distinguisher can conduct in theory. An important property of the trace distance is that any physical operation cannot increase this distance, i.e., the upper bound remains the same even if the distinguisher applies any physical operation.

On side channels of QKD implementations (current status of the theory and experiment) (1)

Trojan horse attacks

Loophole: In 2001 [1] and further in 2006 [2] one realized that bright lasers could be used to probe the internal status of QKD implementation.

Countermeasure: Use a detector to reveal such bright lasers. This is for instance implemented by ID Quantique. Or, one may use an optical isolator with sufficient enough attenuation of the incoming bright light.

Detector efficiency mismatch attacks

Loophole: In 2006 one discovered that timing differences in the detectors could be exploited [3]. In 2007, one of the attacks, the time-shift attack [4] was demonstrated on a commercial QKD system [5].

Countermeasure: A hardware countermeasure was immediately proposed. Furthermore, the loophole is now also covered by security proofs [6-9].

[1] A. Vakhitov *et al.*, J. Mod. Opt 48, 2023-2038 (2001)
[2] N. Gisin *et al.*, Phys. Rev. A 73, 022320 (2006)
[3] V. Makarov *et al.*, Phys Rev. A 74, 022313 (2006)
[4] B. Qi *et al.*, Quant. Inf. Comp. 7, 73-82 (2007)
[5] Y. Zhao *et al.*, Phys. Rev. A 78, 042333 (2008)
[6] C.-H. Fung *et al.*, Quant. Inf. Comp. 9, 131-165 (2009)
[7] L. Lydersen *et al.,* Quant. Inf. Comp. 10, 0060 (2010)
[8] Ø. Marøy *et al.,* Phys. Rev. A 82, 032337 (2010)
[9] L. Lydersen *et al.*, Phys. Rev. A 83, 032306 (2011)

On side channels of QKD implementations (current status of the theory and experiment) (2)

Phase-remapping attack

Loophole: In send-return systems, the eavesdropper can manipulate the source of Alice through timing the pulses from Bob [1]. The attack was implemented on a commercial QKD system in 2010 [2].

Countermeasure: Updated security proofs for this loophole [3-5].

Blinding attacks

Loophole: The detectors can be blinded and controlled by bright light [6-7]. The loophole was proved for two commercial QKD systems [7].

Countermeasure: The research community has proposed several hardware countermeasures [8, 9]. Furthermore, the QKD producers notified this loophole prior to the publication, and implemented countermeasures before the loophole was made public.

[1] C.-H. Fung *et al.*, Phys. Rev. A 75, 032314 (2007)
[2] F. Xu *et al.*, New J. Phys. 12, 113026 (2010)
[3] D. Gottesman *et al.*, Quant. Inf. Comp. 4, 325-360 (2004)
[4] H. Inamori *et al.*, Eur. Phys. J. D 41, 599-627 (2007)
[5] Ø. Marøy *et al.*, Phys. Rev. A 82, 032337 (2010)
[6] V. Makarov, New J. Phys 11, 065003 (2009)
[7] L. Lydersen *et al.*, Nat. Photonics 4, 686-689 (2010)
[8] Z. Yuan *et al.*, Nat. Photonics 4, 800-801 (2010)
[9] L. Lydersen *et al.*, Phys. Rev. A 83, 032306 (2011)

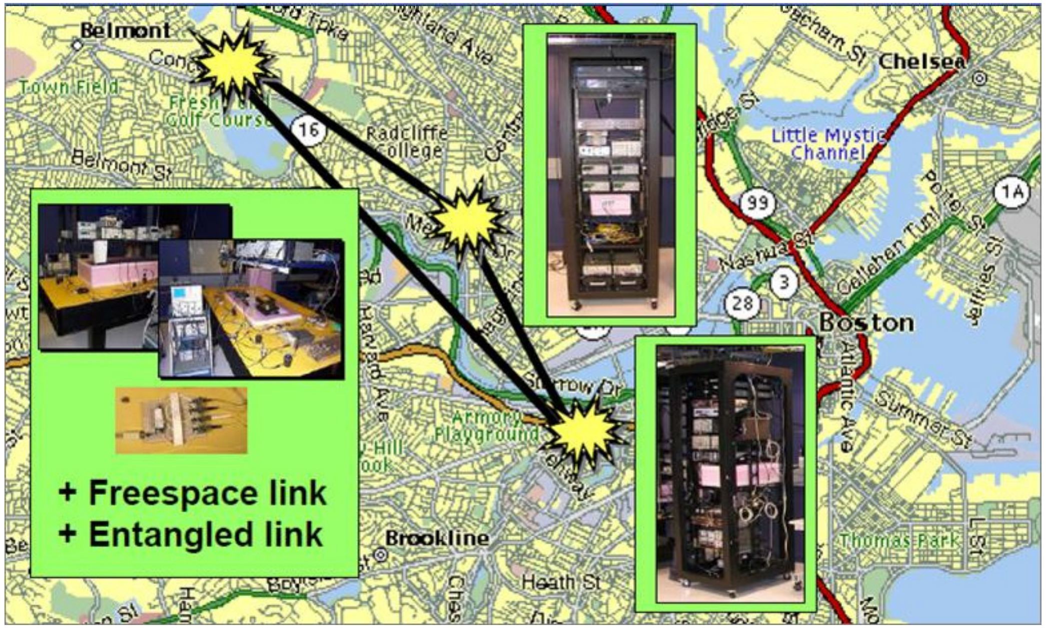
Examples of use cases of QKD

DARPA network (2005)

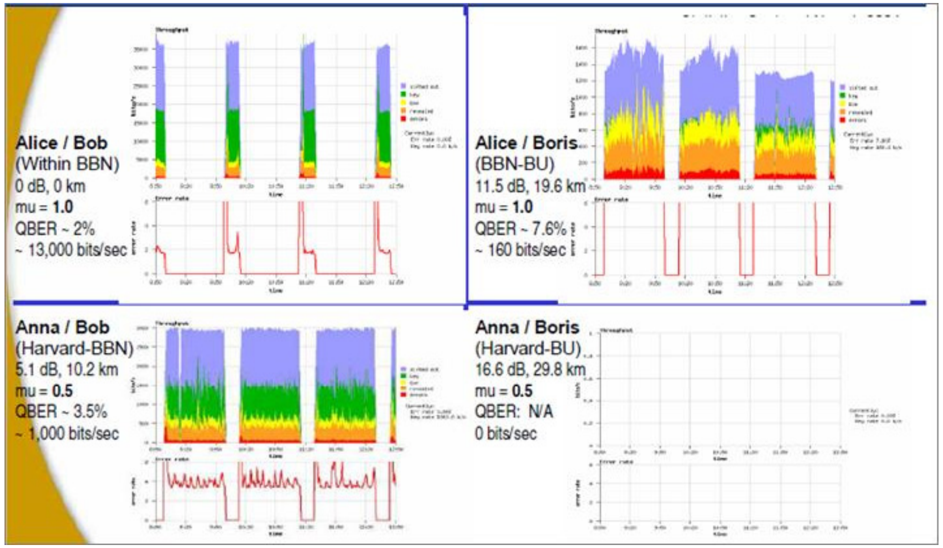
The world's first quantum cryptography network10 nodes in 2005.

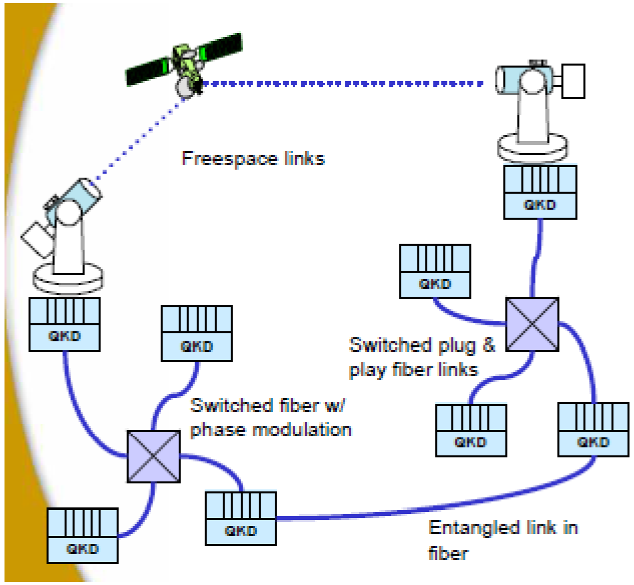
Collaboration between
Harvard University, Boston University and BBN Technology

Secure key rate : 500 bps
Average length :10 km

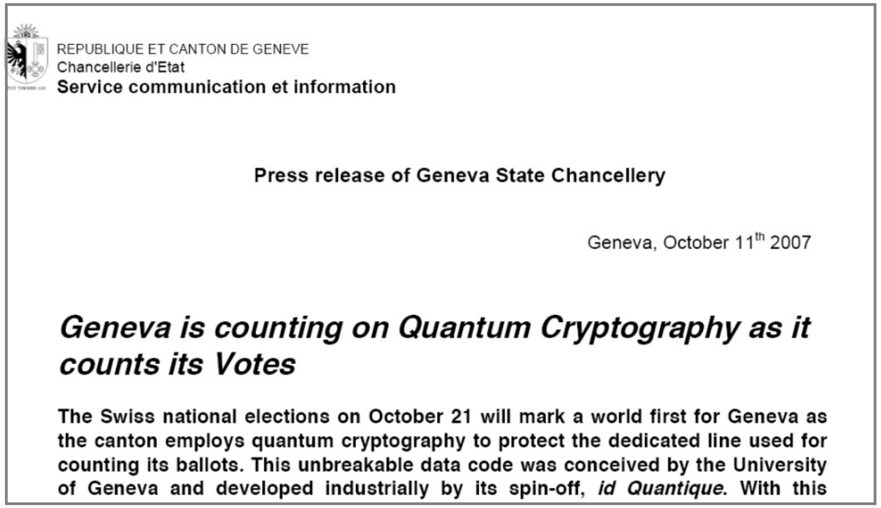


C. Eliott, arXiv:0412029v1 (2004)




Freespace links
QKD
Switched plug & play fiber links
Switched fiber w/ phase modulation
Entangled link in fiber

QKD secures Elections in Geneva



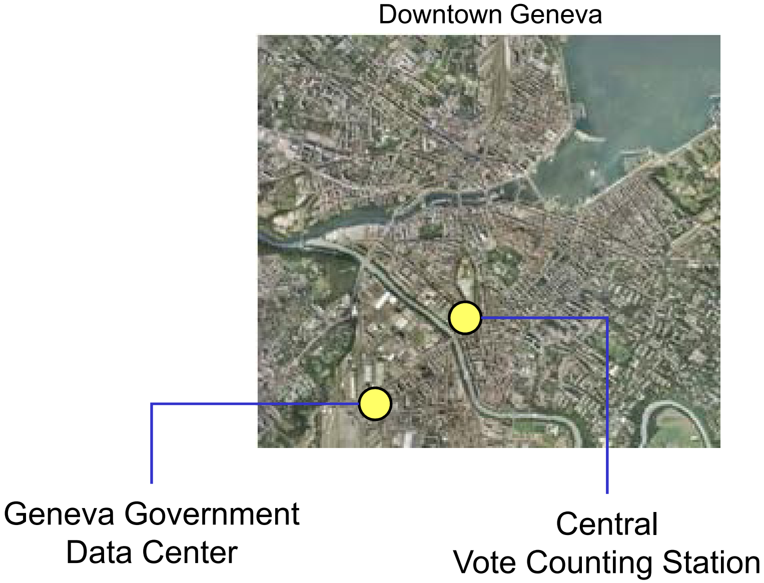
REPUBLIQUE ET CANTON DE GENEVE
Chancellerie d'Etat
Service communication et information

Press release of Geneva State Chancellery

Geneva, October 11th 2007

Geneva is counting on Quantum Cryptography as it counts its Votes

The Swiss national elections on October 21 will mark a world first for Geneva as the canton employs quantum cryptography to protect the dedicated line used for counting its ballots. This unbreakable data code was conceived by the University of Geneva and developed industrially by its spin-off, *id Quantique*. With this

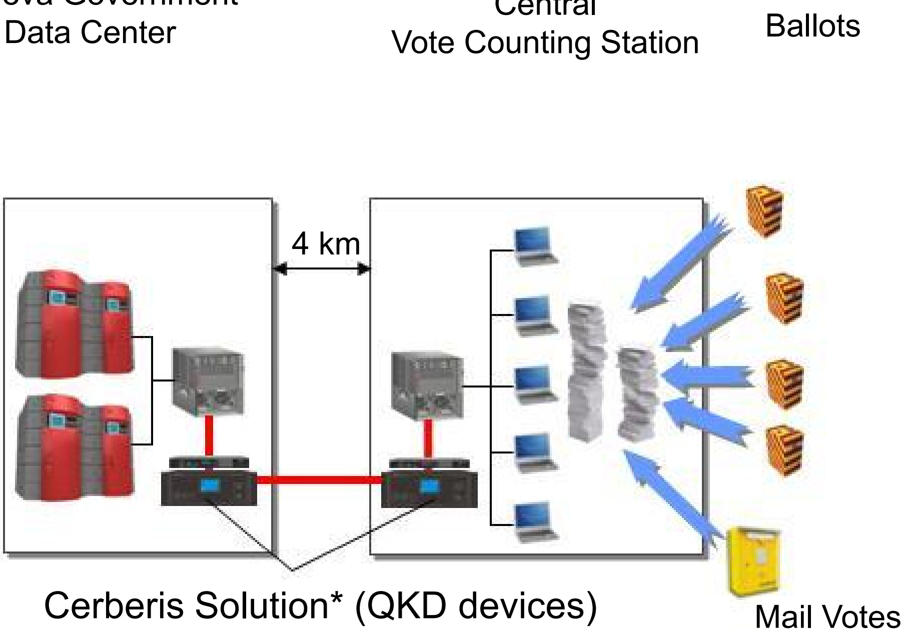


First Deployment:

September 2006 – October 2007,

with election day on October 21st

- **Installation time: 30 minutes**
- **Continuous operation during more than 7 weeks**
- **Encryption of a Gigabit Ethernet link**



Cerberis Solution* (QKD devices)

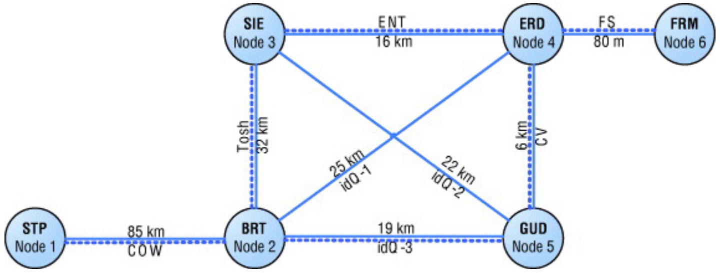
*http://www.idquantique.com/network-encryption/cerberis-layer2-encryption-and-qkd.html

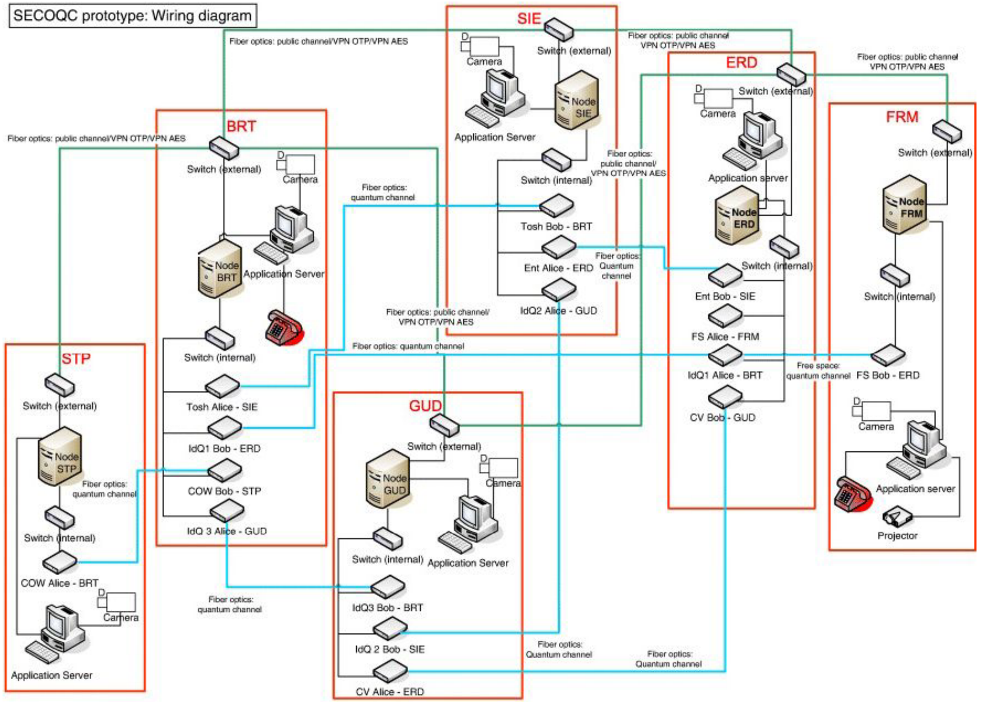
SECOQC (2008)

The SECOQC project:
standardize QKD technology
through a cross-platform interface
allowing the integration on various QKD
systems into one network named
the Quantum Back Borne (QBB)
Network in 2008.

The average link length: 20~30 km
Secure key rate: more than a dozen kbps

6 nodes connected by eight QKD links
Rerouting experiments and
one-time pad encrypted telephone
communication demonstrated.

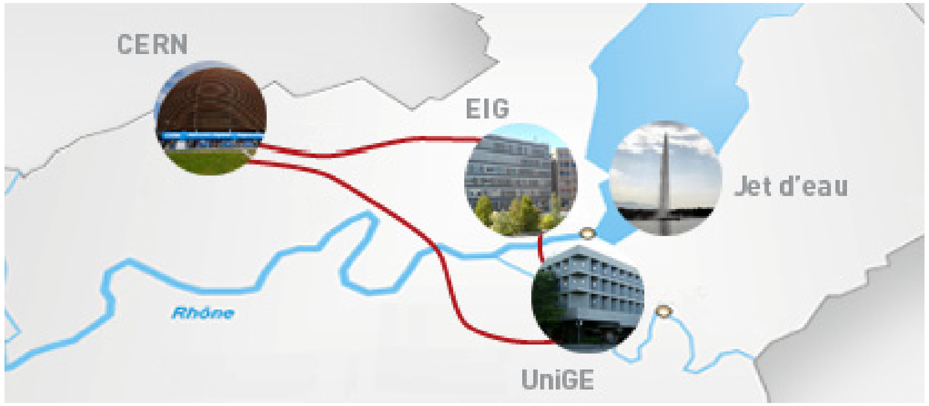




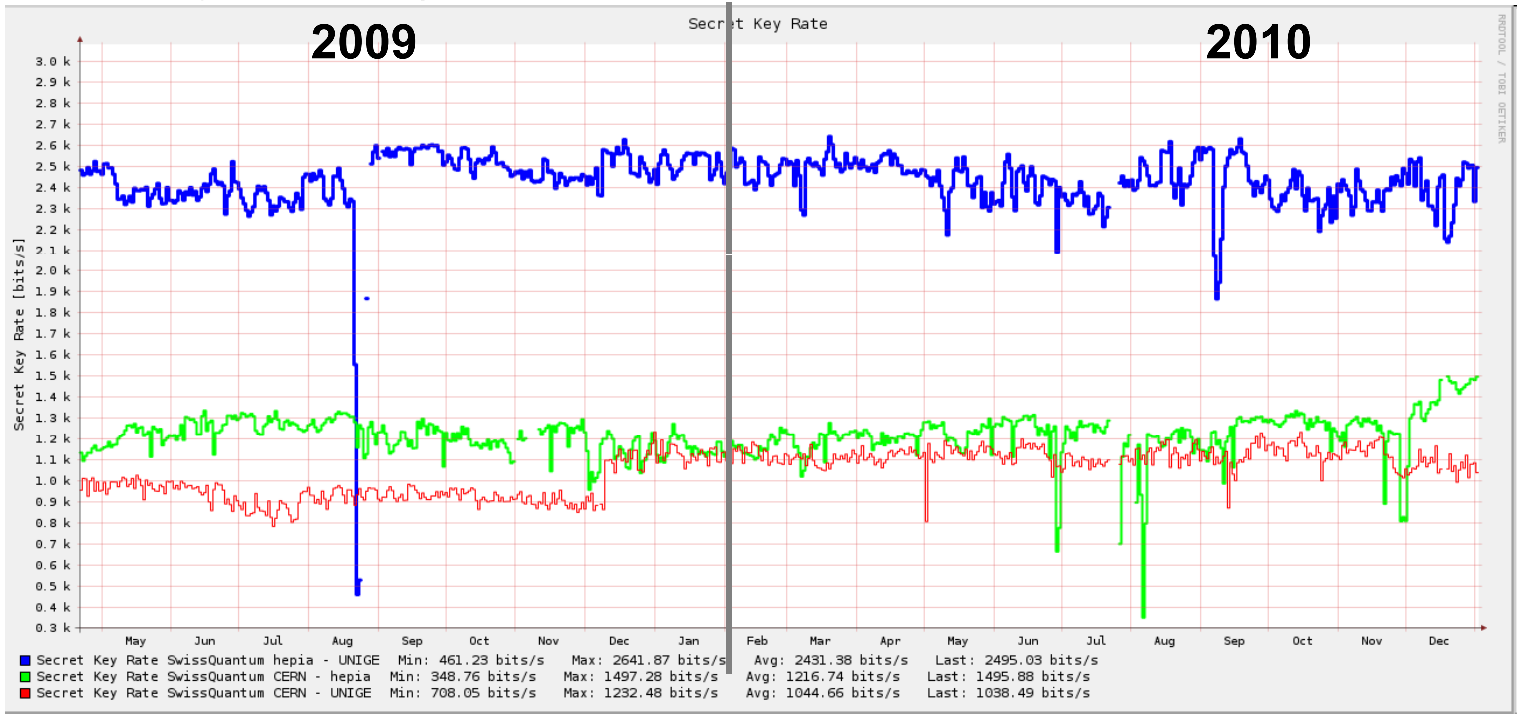
Wiring diagram of the SECOQC protoype.
Blue lines represent quantum channels, green lines—
classical communication

M. Peev et al., New Journal of Physics 11, 075001 (2009)

SwissQuantum (2009-2011)



- University of Geneva is a coordinator of a dozen of partners.
- Deployed for two years in Geneva
- Three links – three nodes
- Links based on Plug&Play QKD
- Cumulated operation time: 45'000+ hours
- Distributed secret bits: 2.5E12
- Key distributions stable with interruptions caused by external factors (power outage, air conditioning failure, etc.)



```
🟦 Secret Key Rate SwissQuantum hepia - UNIGE  Min: 461.23 bits/s   Max: 2641.87 bits/s  Avg: 2431.38 bits/s  Last: 2495.03 bits/s
🟩 Secret Key Rate SwissQuantum CERN - hepia  Min: 348.76 bits/s   Max: 1497.28 bits/s  Avg: 1216.74 bits/s  Last: 1495.88 bits/s
🟥 Secret Key Rate SwissQuantum CERN - UNIGE  Min: 708.05 bits/s   Max: 1232.48 bits/s  Avg: 1044.66 bits/s  Last: 1038.49 bits/s
```

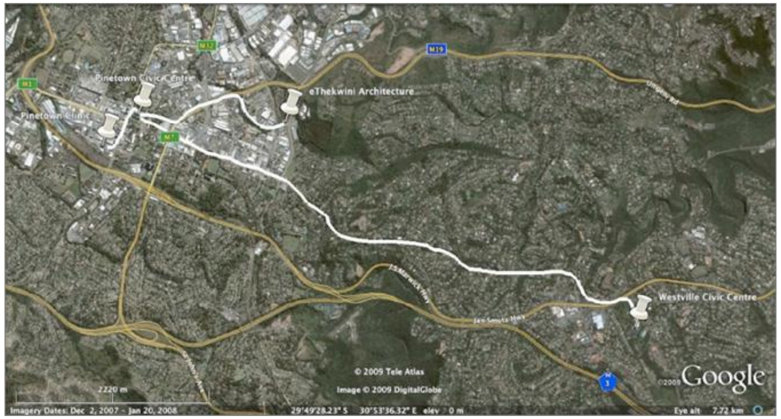
http://swissquantum.idquantique.com/

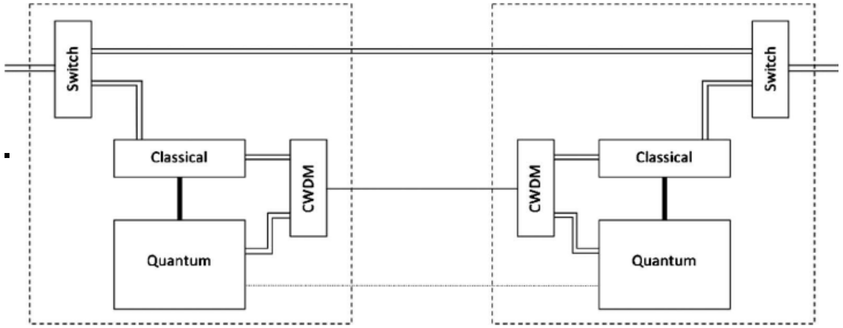
South Africa (2009)

National Institute of Theoretical Physics in 2009
The Durban–QuantumCity project:
a four-node star network

BB84 “plug & play”
Distance: 2.6~27 km
Secure key rate: 891 bps (2.6 km)

This link was used by the eThekwini Municipality during the FIFA World Cup in 2010.





A schematic of the physical connection between links in the QuantumCity project

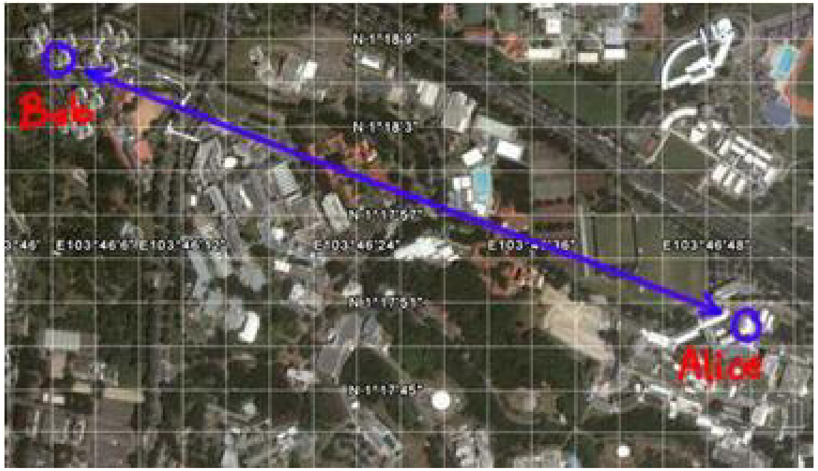
A. Mirza et al., JOSA B, 27, 185 (2009)

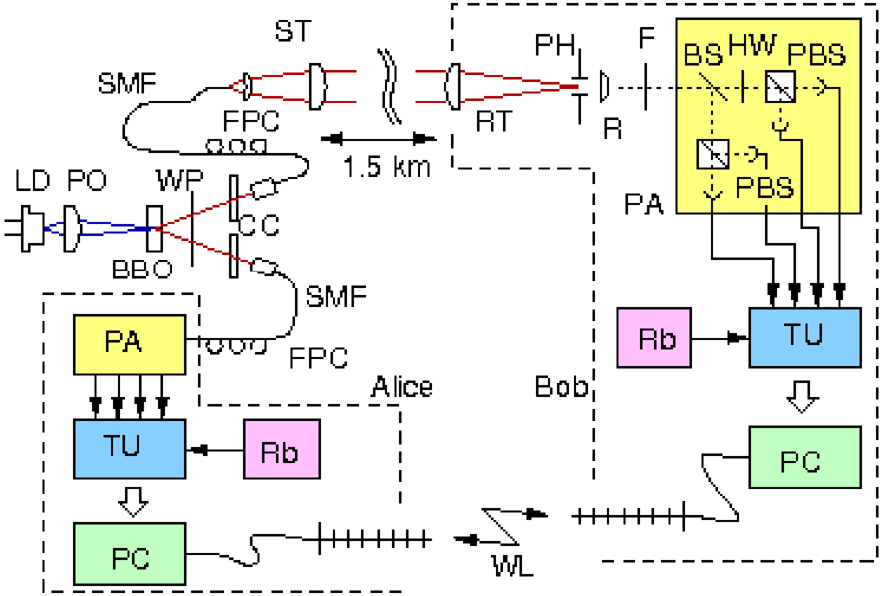
Singapore (2009)

National University of Singapore in 2009

Free space entanglement QKD system over several full day–night cycles

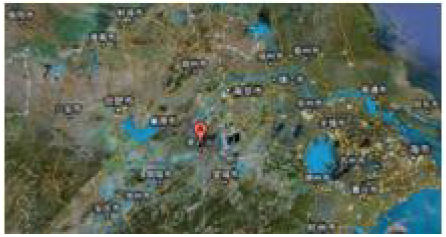
Distance: 1.5 km
Secure key rate: 385 bps



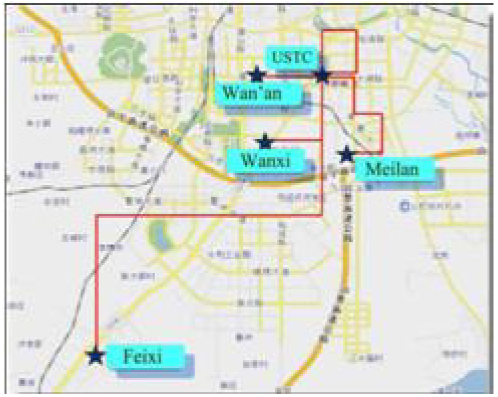


M. P. Peloso et al., New Journal of Physics 11, 045007 (2009)

Projects in China (2009)



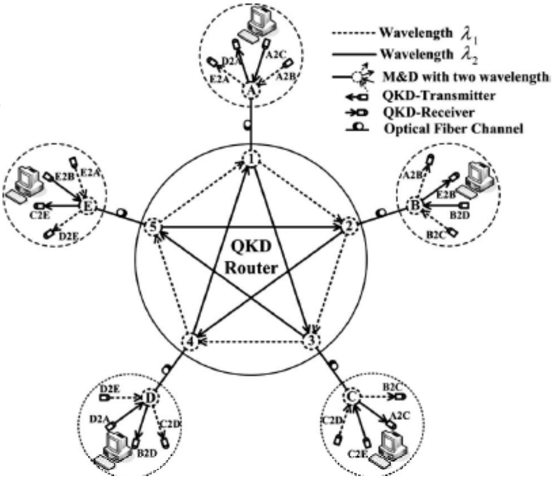
The University of Science and Technology of China in 2009
A metropolitan all-pass quantum communication network in field fiber for four nodes
The average secure key rate: a few kbps (10~60 km)



T-Y. Chen et al., OPT. EXPRESS,18, 27223 (2010)

Metropolitan all-pass quantum communication network constitutes 4 nodes

The University of Science and Technology of China in 2010
Five nodes connected with two wavelengths (1530, 1550 nm)
Every two nodes can share secure keys at the same time
Average attenuation: 10dB
Secure key rate: 2~3 kbps



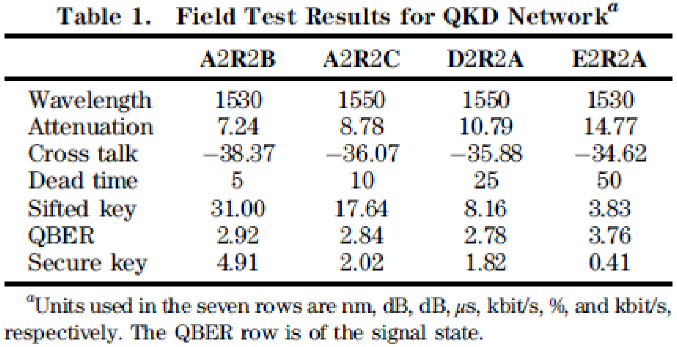
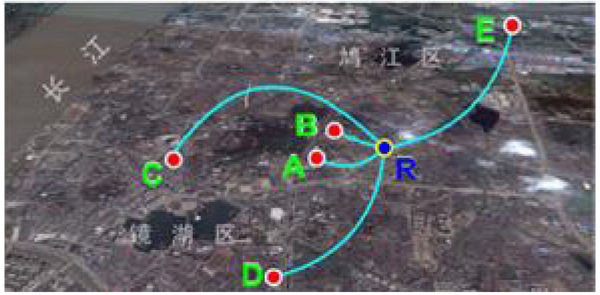


Table 1. Field Test Results for QKD Network[a]

	A2R2B	A2R2C	D2R2A	E2R2A
Wavelength	1530	1550	1550	1530
Attenuation	7.24	8.78	10.79	14.77
Cross talk	−38.37	−36.07	−35.88	−34.62
Dead time	5	10	25	50
Sifted key	31.00	17.64	8.16	3.83
QBER	2.92	2.84	2.78	3.76
Secure key	4.91	2.02	1.82	0.41

[a] Units used in the seven rows are nm, dB, dB, μs, kbit/s, %, and kbit/s, respectively. The QBER row is of the signal state.

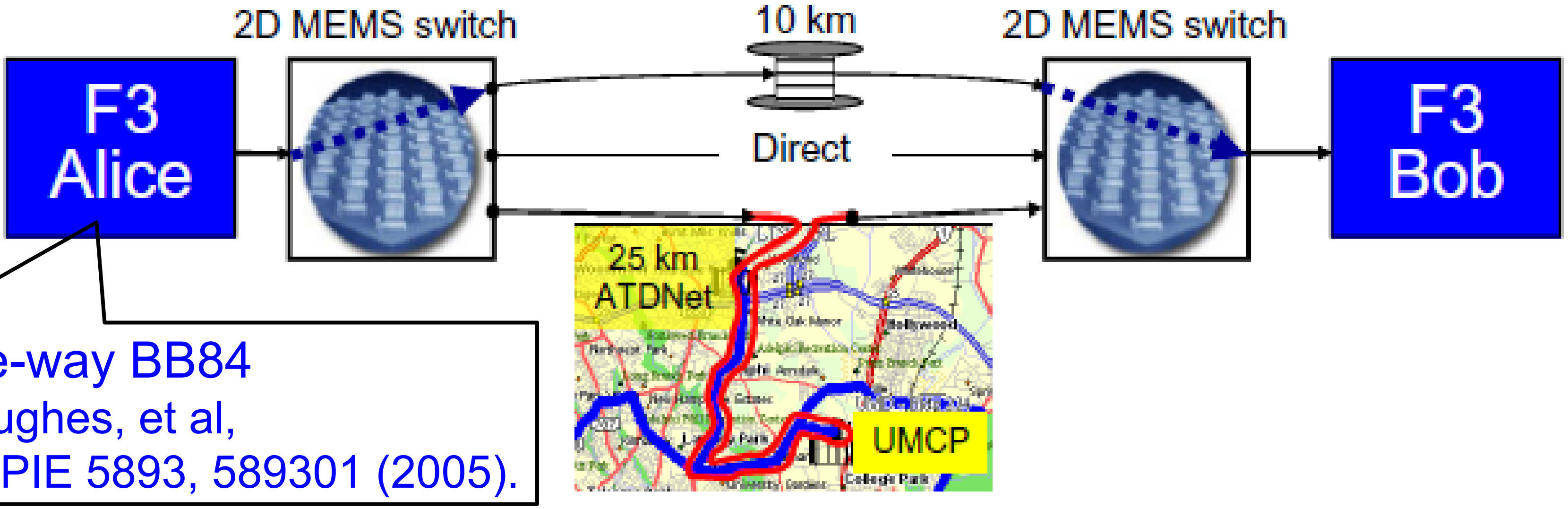


S. Wang et al., OPT. Lett.,35, 2454 (2010)

Dynamically reconfigurable QKD network
in the Washington D.C. area

by Telcordia, Lab. Telecom Sciences, LANL, Naval Res. Lab

Switching and routing of quantum signals into 3 different paths



Secure key rate ~3 kbps
(QBER 3.5%)

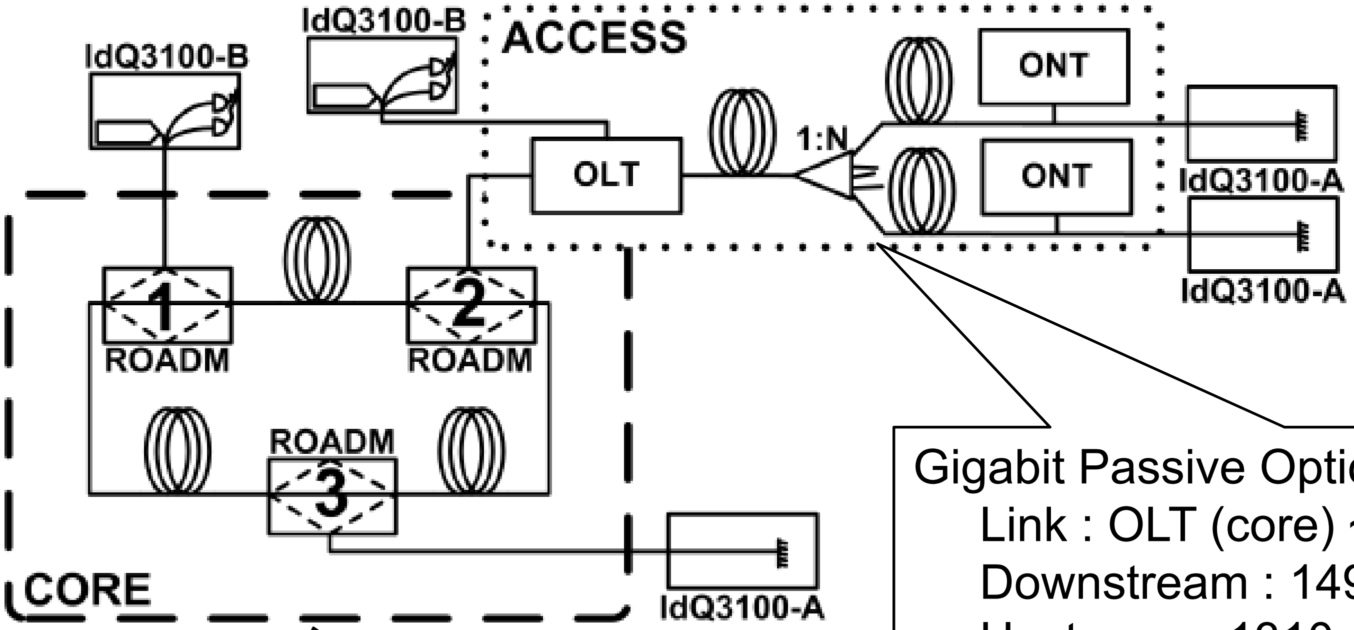
F3 : One-way BB84
R. J. Hughes, et al,
Proc. SPIE 5893, 589301 (2005).

T.E. Chapuran, et al. New J. Phys. 11(10), 105001 (2009).

QKD Network in Madrid

Passive optical network consisting core ring and access networks

D. Lancho, et al., arXiv:1006.1858,



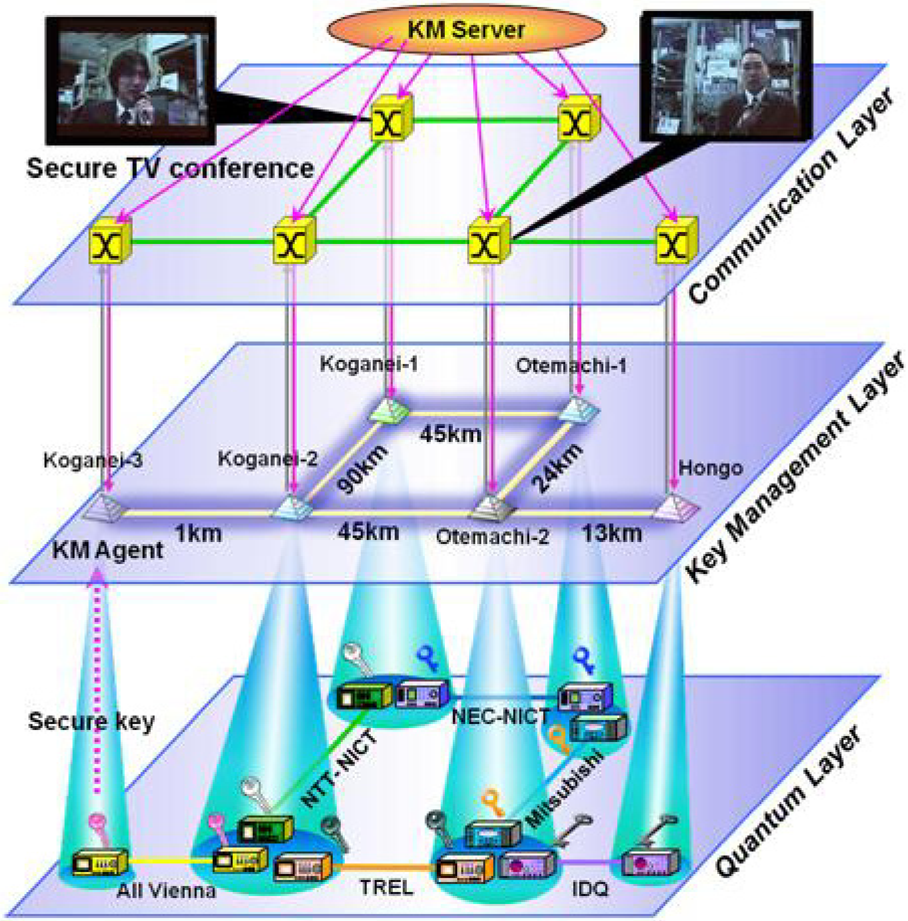
Gigabit Passive Optical Network (GPON)
Link : OLT (core) ~ ONT (client)
Downstream : 1490 nm
Upstream : 1310 nm
QKD : 1550 nm

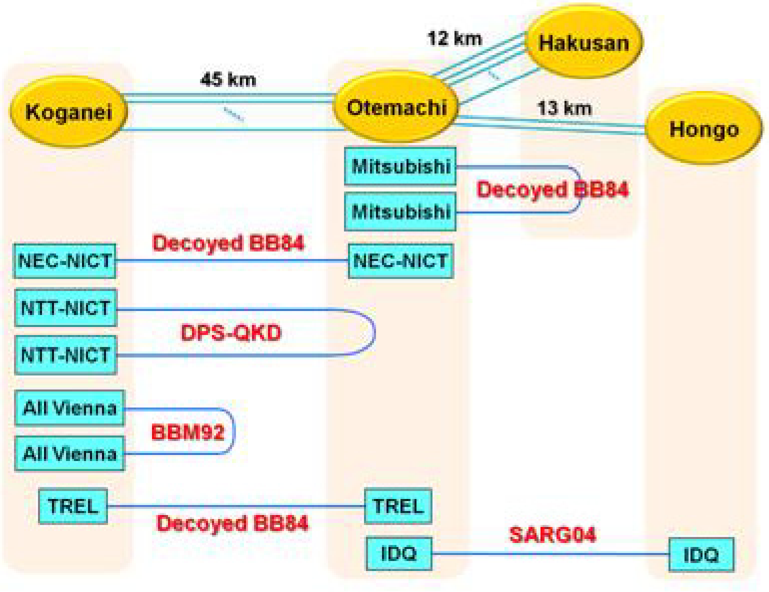
WDM technology and three reconfigurable optical add-drop multiplexers (ROADMs).
1510nm and 1470nm wavelengths are used for classical signals, while 1550nm is reserved for the quantum channel.

Tokyo QKD Network (2010)

Novel GHz-clocked QKD systems, a QKD smart-phone, a reliable commercial QKD product, and an entanglement QKD system were interconnected via several key management agents using a common API, and managed by a single key management server. The demonstrated applications include secure TV conferencing using QKD-OTP and QKD smart-phone. The secure TV conferencing was supported by two relayed QKD routes, each of which includes one trusted relay node, and by a rerouting function to switch from a hacked to an alternative secure link when an eavesdropper in the system was detected. These demonstrations suggest that practical applications of QKD in a metropolitan network may be just around the corner.

arXiv:1103.3566 [quant-ph]
UQCC2010, http://www.uqcc2010.org/


KM Server
Secure TV conference
Communication Layer
Koganei-1
Otemachi-1
Koganei-3
Koganei-2
45km
90km
24km
Hongo
KM Agent
1km
45km
Otemachi-2
13km
Key Management Layer
Secure key
NEC-NICT
NTT-NICT
Mitsubishi
All Vienna
TREL
IDQ
Quantum Layer


12 km
Hakusan
45 km
Koganei
Otemachi
13 km
Hongo
Mitsubishi
Mitsubishi
Decoyed BB84
NEC-NICT
Decoyed BB84
NEC-NICT
NTT-NICT
DPS-QKD
NTT-NICT
All Vienna
BBM92
All Vienna
TREL
Decoyed BB84
TREL
IDQ
SARG04
IDQ