International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Technical Report

(24 November 2021)

ITU-T Focus Group on Quantum Information Technology for Networks (FG QIT4N)

FG QIT4N D1.2

Quantum information technology for networks use cases: Network aspects of quantum information technologies

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

Quantum information technology (QIT) is a class of emerging technology that improves information processing capability by harnessing principles of quantum mechanics which is expected to have a profound impact to ICT networks.

The ITU Telecommunication Standardization Advisory Group established the ITU-T Focus Group on Quantum Information Technology for Networks (FG QIT4N) in September 2019 to provide a collaborative platform to study the pre-standardization aspects of QITs for ICT networks.

The procedures for establishment of focus groups are defined in Recommendation ITU-T A.7.

Deliverables of focus groups can take the form of technical reports, specifications, etc., and aim to provide material for consideration by the parent group in its standardization activities. Deliverables of focus groups are not ITU-T Recommendations.

FG QIT4N concluded and adopted all its Deliverables as technical reports on 24 November 2021.

Number	**Title**
FG QIT4N D1.1	QIT4N terminology: Network aspects of QITs
FG QIT4N D1.2	QIT4N use cases: Network aspects of QITs
FG QIT4N D1.4	Standardization outlook and technology maturity: Network aspects of QITs
FG QIT4N D2.1	QIT4N terminology: QKDN
FG QIT4N D2.2	QIT4N use cases: QKDN
FG QIT4N D2.3	QKDN protocols: Quantum layer
FG QIT4N D2.3	QKDN protocols: Key management layer, QKDN control layer and QKDN management layer
FG QIT4N D2.4	QKDN transport technologies
FG QIT4N D2.5	QKDN standardization outlook and technology maturity

The FG QIT4N Deliverables are available on the ITU webpage, at https://www.itu.int/en/ITU-T/focusgroups/qit4n/Pages/default.aspx.

For more information about FG QIT4N and its deliverables, please contact tsbfgqit4n@itu.int.

Technical Report FG QIT4N D1.2

Quantum information technology for networks use cases: Network aspects of quantum information technologies

Summary

This technical report is a deliverable of the ITU-T Focus Group on Quantum Information Technology for Networks (FG QIT4N). It sorts and analyses QIT for network use cases gathered during the lifetime of the ITU-T Focus Group on Quantum Information Technology for Networks (FG QIT4N).

The uses cases which are only applied by QITs are collected, investigated and summarized; all use cases are analysed by current bottlenecks, application scenarios, technical requirements and solutions. This Technical Report also provides analyses and suggestions for future applications and potential standardization requirements.

Note

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

Keywords

Network aspects of quantum information technology; Use cases.

Disclaimer

The editors have reviewed use cases that were submitted to FG QIT4N. The inclusion of use cases does not imply any endorsement of or judgment on the quality or applicability of the mentioned use cases.

Sample projects, reference articles, specific companies, products or services mentioned in this report are only for the purposes of technical analysis of the use cases. Their mention does not imply that the use cases and their technical aspects are endorsed or recommended by ITU, ITU's Secretariat, the Focus Group or the editors of this report, in preference to others of a similar nature that are not mentioned.

Chief editor: Yuan Gu
ZTE Corporation
China
Email: gu.yuan@zte.com.cn

Co-editors: JiDong Xu
Hengtong Group
China
Email: xujid@htgd.com.cn

Meng Zhang
China Academy of Information and
Communications Technology (CAICT)
China
Email: zhangmeng@caict.ac.cn

Acknowledgments

The editors express their appreciation to all the contributors of this report and all participants of Working Group 1 of the Focus Group on Quantum Information Technology for Networks (FG QIT4N) for their invaluable inputs, thorough review and all comments provided during the development of this report.

Table of Contents

Technical Report FG QIT4N D1.2

Quantum information technology for networks use cases: Network aspects of quantum information technologies

1 Scope

This Technical Report studies the use cases of network aspects of quantum information technology (QIT) under three categories as follows:

- **QIT use cases based on quantum information networks (QINs):** QIT use cases that depend on QIN to realize their function as for example, but not exclusive, to distributed quantum computing, distributed quantum sensing, quantum clock network, etc.
- **QIT use cases beneficial for classic networks:** QIT use cases that can provide additional functionality, new characteristics, or improved performance for classic ICT networks as for example, but not exclusive to, quantum random number generator (QRNG), quantum time synchronization (QTS), quantum cryptography beyond QKD, etc.
- **QIT use cases where the network plays an intrinsic role for the QIT application:** QIT use cases in which the QIT application is significantly defined or enhanced by the functionality provided by a QIN and/or a classical network and is beyond simple remote access of a QIT application via a classical network. Some examples include synchronization of quantum clocks, distributed QRNG beacons for smart contracting, etc.

NOTE – QIN could be defined as any network that incorporates quantum communication technologies for the purpose of transporting quantum states.

In particular, the content of this Technical Report includes use cases of the network aspects of QIT in various relevant fields of application and provides an analysis of their technical advantages, key enabling technologies, maturity and application prospects.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Technical Report uses QIT-related terms in [b-QIT4N D1.1].

3.2 Terms defined in this Report

This Technical Report defines the following terms:

3.2.1 Quantum time synchronization network (QTSN): the network only transmits quantum time synchronization information

3.2.2 Quantum time synchronization information (QTSI): the information contains only quantum time synchronization information

4 Abbreviations and acronyms

This Technical Report uses the following abbreviations and acronyms:

BIPM	Bureau International des Poids et Mesures
BQC	Blind Quantum Computing

COM	Center of Mass
DIQRNG	Device Independent Quantum Random Number Generator
DML	Distributed Machine Learning
DQC	Distributed Quantum Computing
EC	Entangled Clock
ELS	Entanglement Light Source
HOM	Hong-Ou-Mandel
IoT	Internet of Things
LO	Local Oscillator
NISQ	Near-Term Intermediate Scale Quantum Computing
PTP	Point to Point
QA	Quantum Annealing
QAOA	Quantum Approximate Optimization Algorithm
QC	Quantum Computing
QCC	Quantum Cloud Computing
QIN	Quantum Information Network
QIT	Quantum Information Technology
QML	Quantum Machine Learning
QND	Quantum Non Demolition
QRNG	Quantum Random Number Generator
QTS	Quantum Time Synchronization
QTSI	Quantum Time Synchronization Information
QTSN	Quantum Time Synchronization Network
Qubit	Quantum bit
RDMA	Remote Direct Memory Access
SPDC	Spontaneous Parameter Down Conversion
SQL	Standard Quantum Limit
TAI	International atomic time
UC	Use Case
VQA	Variation Quantum Algorithm
VQE	Variation Quantum Eigen solver

5 Introduction

This Technical Report elaborates on use cases of the network aspects of QIT submitted during the lifetime of the ITU-T Focus Group on Quantum Information Technology for Networks (FG QIT4N).

The use cases described in this report provide sufficient detail on the following aspects at a level that is understandable by readers who are not experts in this specific field:

- **Problem statement:** Describes an existing and relevant problem that a specific use case addresses from an end user's perspective.
- **Use case description:** Provides more detail on the application background of the use case, typical application scenarios or fields, etc. It also identifies the target end users of a given use case. An end user can be, e.g., an individual, organization, administrative entity, a commercial company, or combination(s) of these.
- **Motivation/advancement:** Describes the limitations and/or problems of the most relevant current solution(s) of the use case and clarifies how the application of quantum technology to a use case provides a technical advantage and other possible benefits.
- **Technical solution:** Provides a high-level description of the quantum technology-based solution, explaining its functional architecture, modes of operation, etc. Also discusses the challenges of the quantum technology solution, particularly compared to a standard solution (if available).
- **Application prospects:** Discusses the relevance of the use case (importance and frequency) and the existence of alternative solutions that solve the same problem. Also assesses the general cost structure and applicability to certain markets (public, administrative, military) estimating the size of the potential market.

Moreover, this Technical Report summarizes key findings, suggestions for further application and standardization requirements and provides a repository of all collected use cases in Appendix I.

6 Use cases

6.1 Quantum time synchronization use cases

Quantum time synchronization (QTS) describes how quantum technology can be used to achieve high-precision or secure and reliable frequency/time synchronization. The following QTS use cases are provided in this Technical Report:

- **UC-QTS-001** describes the applicability of QTS technology in existing communication networks to achieve ultra-high precision time synchronization. This technology has the potential to evolve into quantum networks in the future.
- **UC-QTS-002** describes the applicability of quantum technology in resisting security attacks in synchronous networks.
- **UC-QTS-003** describes the applicability of quantum frequency/time synchronization technology in quantum star networks. Frequency and time information can be transmitted using entangled qubits and auxiliary classical channels in quantum networks. All nodes in the quantum network can then achieve frequency/time synchronization.

6.1.1 UC-QTS-001: Quantum time synchronization in telecommunications

6.1.1.1 Use case description

Quantum time synchronization provides a high precision time reference from clock source/time server through communication network nodes to end devices/systems (e.g., base stations) for specific applications.

Target end users for UC-QTS-001 include telecommunication operators and time service centres.

6.1.1.2 Problem statement

For 5G, the time synchronization classes are Class A+ 65 ns; Class A 130 ns; Class B 260 ns and Class C 3 us (same as 4G) [b-3GPP]. Based on the time synchronization performance of a device standardized in ITU-T Recommendations in the G.827x series, Class B and Class C can be met, but Class A and Class A+ cannot. For 6G, according to [b-FCC], the working frequency band is 95GHz to 3THz, and the corresponding time synchronization accuracy is on ps level.

As applications evolve, high accuracy of time synchronization is required and, since positioning is an important scenario in the development of IoT, positioning requires much higher time synchronization accuracy, i.e., 1 meter positioning accuracy = 3 ns time synchronization accuracy.

Based on these requirements, a ps level of time synchronization accuracy is needed. However, current technical solutions (e.g., PTP) can only achieve ns level of time synchronization accuracy.

6.1.1.3 Motivation/advancement

Current technical solutions (e.g., PTP) can only achieve ns level of time synchronization accuracy in typical telecommunication networks which have many nodes (e.g., 20 nodes in simulation module as standardized in ITU-T Recommendations in the G.827x series). As applications evolve, there may be a big network with more nodes in the future and it is unlikely to meet the time synchronization accuracy by reducing the number of nodes.

QTS can use a quantum technology-based clock source and/or quantum states (or Qubits) and entangled state transmission to achieve high precision time synchronization between different nodes [b-Giovannetti-1]. Since a quantum state has its own clock, its transmission process is not affected by the transmission medium. If the entangled state is used to synchronize two clocks, it would have nothing to do with the initial phase of the two clocks [b-Ebubechukwu]. The fundamental source of error in the QTS would be due to the imperfect entanglement that is distributed between two nodes, and the quantum noise due to the standard quantum limit in the QTS protocol itself. The error in the QTS obeys a relation as in Equation (1) [b-Ebubechukwu]:

$$\delta\mathrm{t} \approx \frac{1}{\omega}\sqrt{\frac{2^n}{N} + 1 - F_n} \tag{1}$$

where ω is the clock frequency, N is the number of available Bell pairs for quantum time synchronization, n is the number of rounds of purification performed, and F_n is the fidelity of the Bell pairs after n rounds of purification.

For a Cesium (Cs) clock, its reference frequency is 9.192631770 GHz which corresponds to ω_{Cs}^{-1}=17 ps. If $F_0 \approx 0.9$ and N = 10^5 are selected, then the corresponding δt ≈ 5.4ps.

If the most accurate Strontium (Sr) clock is selected, the reference optical frequency transition frequency value is 429.228004229873 THz which corresponds to ω_{Sr}^{-1}= 0.4 fs. If $F_0 \approx 0.99$ and N = 10^8 are selected, then the corresponding δt = 0.04fs.

The new characteristics of these quantum states enable the accuracy of QTS to surpass the insurmountable obstacles of classical time synchronization accuracy, achieve unprecedented high accuracy, and meet the demand for high-precision time synchronization in the future.

Therefore, quantum synchronization technology that can achieve higher time synchronization accuracy (i.e., ps/fs) could be applied making use of the security of quantum synchronization technology which is an important technical advantage.

6.1.1.4 Technical solution

Quantum synchronization technologies have been studied for a long time and there is a lot of research and published reports which indicate that quantum synchronization technology can achieve ps level, even fs level of time synchronization accuracy.

Two aspects can be considered to improve the time synchronization accuracy of communication networks, i.e., clock source and synchronization protocol.

6.1.1.4.1 Clock source

At present, the most accurate clock source in the world is the atomic clock which is based on the energy level transition of some ions resulting in emitted electromagnetic waves of very stable frequency. Different working substances have different performances of accuracy and they have expanded from Cesium and Rubidium to Strontium and even Mercury.

In 2008, scientists at the National Institute of Standards and Metrology (NIST) developed an atomic clock based on Mercury ions whose accuracy record is 1 second per 1.6 billion years [b-NIST-1], [b-NIST-2]. Its working band is in the optical band (the traditional Cesium atomic clock is in the microwave band) thus it is also called an optical clock. The emitted wavelength of the optical clock is shorter than the Cesium atomic clock, resulting in higher accuracy. Table 1 shows the working frequency and accuracy of different working substances.

Table 1 – Working frequency and accuracy of different working substances

Type	Working frequency (Hz)	Accuracy
^{133}Cs	9 192 631 770 [b-BIPM-1]	10^{-13}
^{87}Rb	6 834 682 610.904 324 [b-BIPM-2]	10^{-12}
^{1}H	1 420 405 751.7667 [b-Essen] and [b-Dupays]	10^{-15}
Optical clock (^{87}Sr)	429 228 004 229 873.4 [b-BIPM-3]	10^{-17}

In the past two decades, more results and great progress has been achieved by scientific projects dealing with optical clocks. However, before optical clocks become a universally adopted clock source/timescale, there are still several issues that need to be studied:

– **Service time of optical clocks:** From minutes to hours, the progress has been very slow. It is not clear what the best current performance is, but optical clocks are significantly more modest than the atomic fountains which are the current primary frequency standards.

– **Comparison between optical clocks:** Currently in practice, there is a low possibility of comparing optical clocks to each other in the same laboratory because very few National Measurement Institute (NMI) laboratories have two optical clocks due to their complexity and cost. Comparing optical clocks remotely is an alternative method, however, due to the high performance in frequency stability (10^{-17} to 10^{-18}), it is not possible to use classical methods for remote comparison (e.g., GNSS methods). Optical clocks need to be compared through networks/fibre links with the frequency stability better than the signals to be compared (i.e., from optical clocks). Several scientific projects have achieved frequency stability of between 10^{-18} and 10^{-20}, but with higher complexity and more costly technical solutions.

– **Distribution of optical clock source reference:** As the performance of optical clocks is extremely high in practice, it will take a long time and significant investments to build distribution networks for new reference signals (with protection features) to serve entire networks. Using quantum states, quantum bits, and entangled state transmission is another possible way to build the distribution network.

Moreover, most research is focused on the conflicting goals of making the clocks smaller, cheaper as well as more portable, energy efficient, accurate, stable and reliable.

6.1.1.4.2 Synchronization protocol

Quantum synchronization protocols use quantum entanglement and high-order correlation characteristics to break through the classic shot noise limit, thereby improving synchronization accuracy. Typical technologies of quantum time synchronization, which are different from classical time synchronization, require the entanglement light source (ELS) and corresponding specific protocol-based methods. The ELS irradiates a nonlinear crystal with a continuous light source or pulse light source to produce entangled photon pairs, one of which is signal light and the other is idle light. The QTS protocol transmits and detects entangled photon pairs through different paths between Alice and Bob, respectively, based on second-order coherence of the entangled photon.

Although there are many QTS protocol-based methods, this technical report focuses on the following three methods:

a. Technical solution 1: Round trip protocol

Alice at A has Clock 1, and Bob at B has Clock 2. The ELS at A prepares the frequency entangled photon pairs. The signal light and idle light respectively arrive at B through two optical paths and reflect back to A where they interfere with each other on the 50:50 splitter and reach photon detectors D1 and D2. The counting rate measured by the coincidence counter is a function of the optical path difference which includes the initial time difference information between Clock 1 and Clock 2, see Figure 1 [b-Giovannetti-2], [b-Giovannetti-3] and [b-Hong].

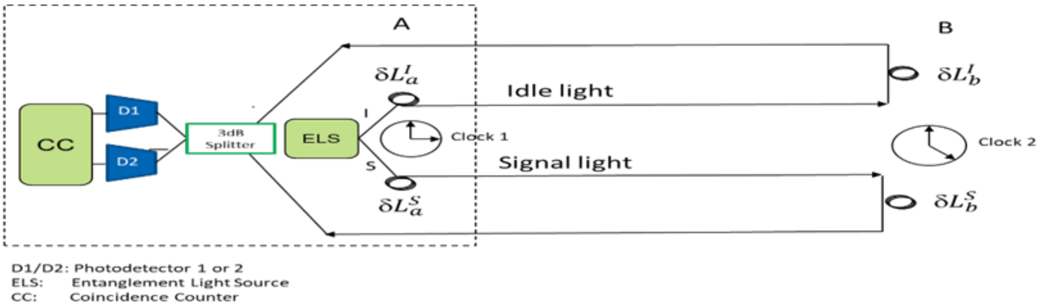


Figure 1 – Round trip protocol principle

In the optical paths between A and B, the delay optical path is set related to time δL_a^I, δL_a^S, δL_b^I, δL_b^S, where δL_a^I , δL_b^S will increase over time and δL_a^S, δL_b^I will decrease over time. By adjusting the time delay and measured light at D1 and D2, these measurement outputs are then sent into coincidence counter measurement known as the Hong-Ou-Mandel (HOM) interferometry measurement [b-Giovannetti-2], or also called second-order quantum interference measurement. The optical path difference of signal and idle light can be obtained by coincidence counter, and the corresponding counting rate is:

$$P_C = \int \mathrm{d}\omega \, |\varphi(\omega)|^2 \left[1 - cos\left(2\frac{\omega}{c}(\delta l_0 - \delta l)\right)\right] \qquad (2)$$

where $\delta l_0 \cong 4\nu\tau,$ ν is delay rate, and $\tau = t_0^a - t_0^b$ is the time difference between Clock 1 and Clock 2.

In the Gaussian spectrum$|\varphi(\omega)|^2$, Equation (2) becomes:

$$P_c = 1 - e^{-2\Delta\omega^2(\delta l - \delta l_0)^2/c^2} \qquad (3)$$

where the function $P_c(\delta l)$ have a dip of width $1/(4\Delta\omega)$ centred in $\delta l = \delta l_0$. The time difference τ between the two clocks can be obtained by measuring the dip position.

The advantage of this time synchronization protocol is that it does not need to measure the arrival time of the signal and avoids the measurement error. Since the signal light and idle light are frequency entangled and their optical path is round trip, the dispersion effect of the fibre will be eliminated.

b. Technical solution 2: One-way protocol

This method is based on the measurement of the entangled photon pair unidirectional time synchronization protocol, i.e., the entangled photon does not need to reflect back and forth, but only needs one-way transmission. The entangled photon source can be placed at the third party or directly at the measurement place A or B. This is based on the measurement of the two-order correlation function of the entangled state. Its basic principle diagram is shown in Figure 2.

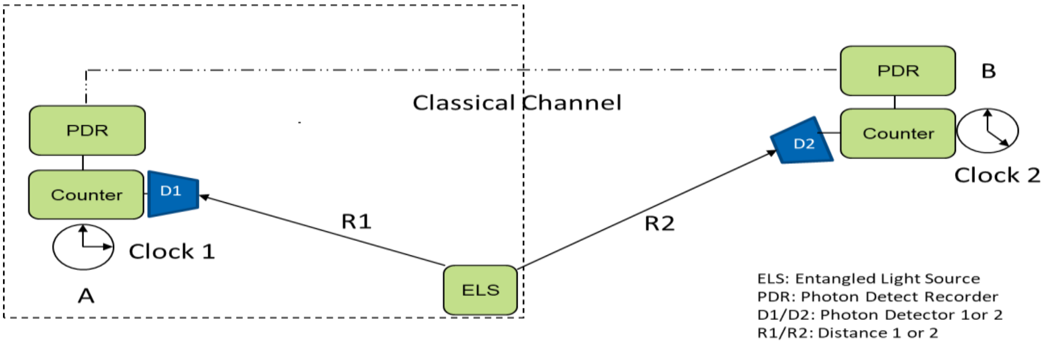


Figure 2 – The one-way protocol principle [b-Valencia]

Clock 1 and Clock 2 which are to be synchronized are located at A and B respectively, where A can be a base station or laboratory on the ground, and B could be another remote base station or a satellite in space. The ELS is located at A and its signal light and idle light going through A and B are detected by photon detectors D1 and D2 respectively, where R1 is the distance between ELS and D1, and R2 is the distance between ELS and D2. The times when photons arrive at the detector are recorded by Clock 1 and Clock 2 as t_1 and t_2, respectively and the recorded time is compared through classical channels. If the two clocks are synchronized, t_1 and t_2 which are obtained by joint measurement of signal light and idle light will satisfy the maximum correlation degree.

ELS sends the signal light to D1 and the idle light to D2 and the time difference t_1-t_2 is:

$$t_1 - t_2 = \frac{R_1}{V_S} + t_0 - \frac{R_2}{V_I} \tag{4}$$

where V_S and V_I are the transmission speed of signal light and idle light respectively, t_0 is the time difference between Clock 1 and Clock 2 (which is also the key parameter for clock synchronization between two nodes).

The signal light is then swapped with the idle light and the signal light is sent to D2 and idle light to D1. The time difference of photon arrival is then as follows:

$$t_1' - t_2' = \frac{R_1}{V_S} + t_0 - \frac{R_2}{V_I} \tag{5}$$

$$\Delta \mathrm{t} = (t_1 - t_2) - (t_1' - t_2') = \mathrm{D}(R_1 - R_2) \tag{6}$$

where $D=1/V_S-1/V_I$.

Since Δt can be measured and R1 is known, R1 can be changed, and the process repeated. Then, R2 and D can be calculated and finally, t_0 can be known by substituting R2 into the formula. The accuracy, however, depends on the measurement accuracy of t_1 and t_2.

This time synchronization protocol is suitable for long distance time synchronization and can also be used for long-distance time service and positioning.

c. Technical Solution 3: Two-way protocol

The equipment architecture of this scheme is mainly based on the Mach-Zehnder interferometer (MZI) structure which sends photons to each other and measures the phase difference to obtain the clock difference [b-Xie]. Compared to the classic scheme, this scheme does not need to transmit the physical clock and measure the pulse arrival time during the synchronization process so, it is not affected by the gravitational potential. The theory proves that it resists the influence of dispersion and can achieve higher accuracy requirements.

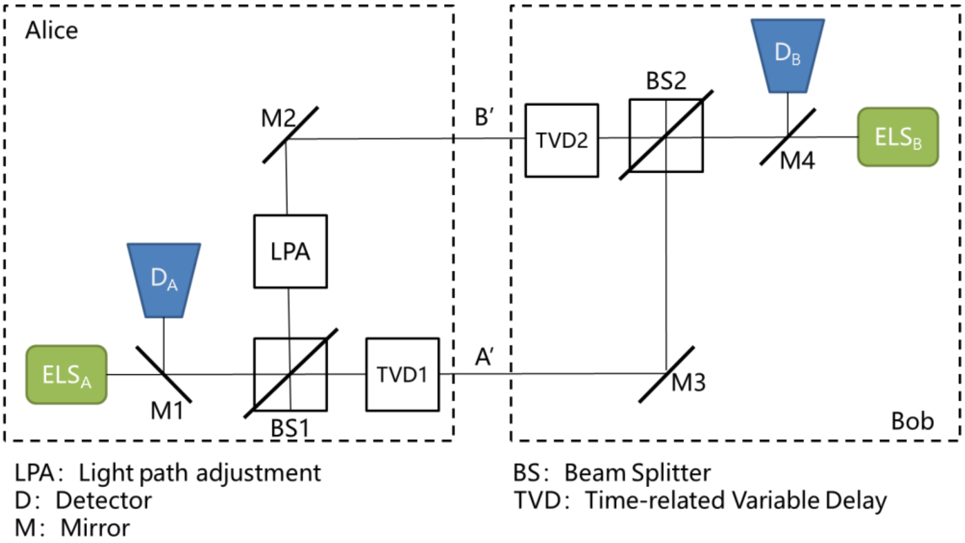


Figure 3 – The two-way protocol principle

First, it is necessary to adjust the optical path to make the two interference arms equal in length. Alice generates entangled photon pairs, one of which is sent to Bob and the other one is used for local detection. If one is detected locally, the counting message is sent to Bob through the classical channel. The other photon passes through the variable delay device 1 or 2 along the path A 'or B'. When Bob detects the photon and receives the count message sent by Alice, he confirms that he has received the photon. Bob generates entangled photon pairs and repeats the process described previously.

The probability of detecting a photon at the detector B/A is:

$$P_{B(A)} = \frac{1}{2} \ (1+\cos\varphi_{AB(BA)}) = \frac{1}{2}(1 + cos\frac{2\pi\Delta L_{AB(BA)}}{\lambda}) \tag{7}$$

where:

$$\Delta L_{AB(BA)} = 2v[\frac{L}{c} + (t_{A(B)} - t_{B(A)})] \tag{8}$$

and v is the rate of delay change.

Solving the above equation gives:

$$\Delta t = t_A - t_B = \frac{\lambda(\varphi_{AB}-\varphi_{BA})}{4\pi v} \tag{9}$$

Compared to the classic scheme, the characteristic of this scheme is that there is no need to transfer the physical clock or measure the pulse arrival time. Through theoretical proof, the synchronization accuracy of the scheme is related to the number of transmitted and received photons. The greater number of photons sent or received in the experiment, the higher the measurement accuracy. Since this scheme can also resist the influence of dispersion effect, theoretically, it can achieve higher accuracy than the classical scheme.

QTS is achieved by the transmission and processing of quantum states (or Qubits) to reach the high-precision time synchronization level. However, quantum bits are incompatible with classical bits and will interfere with each other when transmitted in the same network. Therefore, the best approach is to separate QTS and classical networks into different networks.

QTS network (QTSN) and classical networks can operate independently in the same fibre with WDM method, i.e., different optical working wavelengths are adopted. The situation is similar to the coexistence of QKD network (QKDN) and classical networks, C-band and O-band can be used for classical optical communication and quantum signal respectively to reduce their influence on each other [b-Mao]. QTSN is also independent from QKDN and can coexist with it.

QTSNs can provide more accurate information of time synchronization service. The classical network sends out requests to QTSN through the interface of the same nodes for both networks. The QTSN operates according to the requirements and transmits the synchronized information to the classical network through the node interface. The classical network can correct the time of the clocks at the corresponding network node according to the time synchronized information.

In future QINs, QTS can be carried out directly through the transmission and processing of quantum bits. Quantum time synchronization information (QTSI) which takes up the part of payload expenses in quantum information can be transmitted alternately with quantum information in the same quantum channel. QTSI can be integrated and executed anytime and anywhere according to the demand and both QTSI and quantum information are fully integrated in the QIN. Therefore, there would be no need for a separate QTSN to exist.

The fibre-based optical clock synchronization can be wavelength division multiplexed with quantum communication in a single fibre link while the quantum communication can provide secret keys to encrypt the classical timing data of the clock synchronization which can improve the security of clock synchronization.

6.1.1.5 Application prospects

Synchronization networks are one of the basic networks of communication networks. Current time synchronization networks consist of three parts: time source, time transmission and end application. Improving the time synchronization accuracy can be achieved by using a quantum clock source and/or quantum synchronization protocols in communication networks. With this and the previous description in consideration, the size of the potential market for quantum clock synchronization (QCS) could be estimated at around 100 billion.

6.1.2 UC-QTS-002: Secure quantum clock synchronization

6.1.2.1 Use case description

Security attacks on time synchronization have a serious adverse impact on services that depend on accurate time. Secure quantum clock synchronization is introduced to realize safe and reliable transmission of synchronization information to the end node.

Target end users for UC-QTS-002 include telecommunication operators and time service centres.

6.1.2.2 Problem statement

In recent years, with the introduction of various attacks on the clock synchronization protocol, the security of clock synchronization has received widespread attention. Therefore, when using a clock synchronization protocol outside of a fully trusted network environment, it needs to be protected. The clock synchronization protocol is particularly susceptible to delay attacks because changes in the time at which messages are sent and received can cause errors in the calculation of the clock difference between two nodes. Delayed attacks, in particular, decrease the accuracy of clock synchronization which can cause applications that depend on it to fail. Such attacks can seriously affect time-sensitive network applications.

6.1.2.3 Motivation/advancement

There are two kinds of attacks on synchronous networks (especially those based on PTP protocol):

1) **PTP message attacks** which can be prevented by means of message encryption or authentication. However, the encryption process itself introduces some uncertain delay which leads to the degradation of synchronization performance.

2) **Delay attacks** which cannot be prevented by simple encryption means.

Although quantum clock synchronization technology does not require encryption, and therefore does not introduce uncertain additional delay, there is currently no technical means (QND measurement) that can add asymmetric delays in space without destroying other degrees of freedom. Thus, the above two kinds of security attacks can be prevented.

6.1.2.4 Technical solution

Entangled photon pairs generated by spontaneous parameter down conversion (SPDC) have been widely used in quantum information protocols. Alice and Bob each have a source of polarization entangled pairs generated by SPDC. Each entangled photon pair can be detected by either the local or remote detector. Both Alice and Bob use the local clock to record the moment when the photon is detected and these differences between the time labels can be extracted by calculating a cross-correlation between events at both sides. Such a protocol based on quantum communication technology can provide a verified and secure time synchronization protocol.

Unlike classical protocols designed to improve the security of time distribution, this quantum synchronization protocol does not require any assumptions about the distance or propagation time between clocks. [b-Giovannetti-1] describes a secure quantum clock synchronization scheme as illustrated in Figure 4.

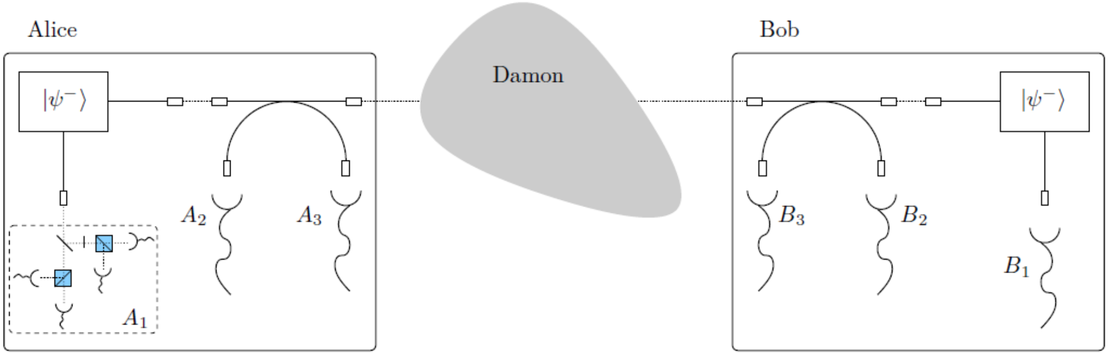


Figure 4 – Secure quantum clock synchronization protocol system [b-Giovanetti-1]

Some basic properties of the entangled photons used to measure the clock offset ensure the security of the protocol. To destroy the security of quantum protocol, an adversary must change the propagation of photons in the single space mode between Alice and Bob, i.e., introduce asymmetric transmission delay. Therefore, one must find a way to measure the propagation direction of photons in the channel, so that:

1) When the direction measurement is successful, one must know the measurement result (or at least have a high probability of knowing), and

2) When the direction measurement is successful, the direction measurement must be non-destructive, i.e., does not destroy photons (for example, being absorbed) and change any other degrees of freedom of photons.

Even though eavesdroppers could potentially master quantum non-demolition (QND) measurement or direct generation of controllable coherent single photon non-reciprocity in future, at present there is no means to do so thus, the quantum clock synchronization protocol is secure when the adversary cannot perform QND measurements on a single photon.

6.1.2.5 Application prospects

Secure quantum clock synchronization is currently in the experimental research stage and does not meet conditions for commercialization.

6.1.3 UC-QTS-003: A quantum network of entangled clocks

6.1.3.1 Use case description

A quantum clock network that uses non-local entangled states can realize shared high precision (near the fundamental precision limit by quantum theory) timing by combining precision metrology and quantum networks for some applications like satellite navigation.

Target end users for UC-QTS-003 include telecommunication operators and time service centres.

6.1.3.2 Problem statement

The standard time generally used around the world is Coordinated Universal Time (UTC), which is produced by the international atomic time cooperation led by BIPM: about 80 punctuality laboratories distributed around the world use more than 500 commodity punctual clocks to generate their own local time. Each laboratory reports the relevant data to BIPM through satellite comparison and weighs all atomic clock data to obtain the free atomic time (evaluation assurance level (EAL)). The frequency reference (PFS) developed by a few countries is used to control and correct the system deviation to generate the international atomic time (TAI) which is corrected by irregular leap seconds to get UTC. The process of weighted average of clock group usually adopts the classical method so that the precision of classical algorithm cannot exceed the standard quantum limit (SQL).

On the other hand, in recent years many new types of synchronous security attacks such as GPS satellite retreat, satellite simulator interference, time source switching caused by PTP disoperation, message attacks and delay attacks against synchronous transmission protocol, etc. have brought many negative impacts on business activities and network operations. With the large-scale construction and operation of 5G networks, the openness of the network and the diversification of service types have made the security problems of synchronization networks increasingly prominent.

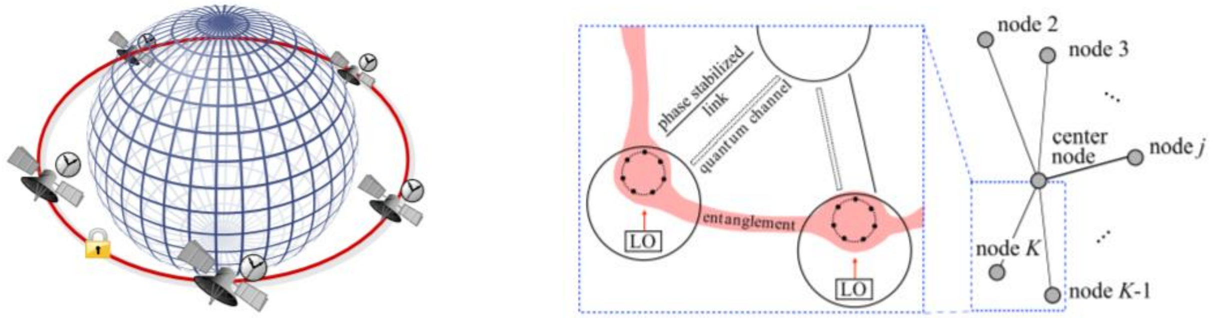
6.1.3.3 Motivation/advancement

The precision of classical algorithm cannot exceed the standard quantum limit (SQL).

One of the advantages of the quantum clock network involves is its ability to maintain and synchronize the time standards across multiple parties in real time. Unlike the current world time standard, where the individual signals from different clocks are averaged and communicated with a time delay (so-called paper clock), all participants in the quantum clock network can have access to the ultra-stable signal at any time. This makes it possible to measure systematic errors of different clocks in real time and allow one to correct them, unlike in the case of the paper clock which has to rely on the retrospectively averaged time signals. The enhanced stability of the network signal hereby allows longer Ramsey times in the control measurements used to determine the systematics of the single clock. Furthermore, by having full access to their local clocks, the different parties keep their full sovereignty and ensure security, as opposed to a joint operation of a single clock.

6.1.3.4 Technical solution

[b-Kómár] describes a quantum-based cooperative protocol for operating a network of geographically remote optical atomic clocks. By using non-local entangled states, an optimal utilization of global resources can be realized. This kind of network can operate near the basic precision limit set by quantum theory. In addition, the internal structure of the network, combined with quantum communication technology, ensures the security against internal and external threats. The realization of such a global quantum clock network can enable a real time single international time scale (World Clock) with unprecedented stability and accuracy to be built.



a) Cooperative clock operation protocol with multiple satellite-based atomic clocks

b) Different nodes employing network-wide entangled states to interrogate their respective LOs.

Figure 5 – The structure of a quantum clock network

As illustrated in Figure 5 (b), the quantum clock network consists of K nodes and each node contains n atoms (qubits). One node is selected to be the centre node which has an additional 2(K-1) ancilla qubits. First, a fully entangled state $\left[|00...0\rangle_{1_1,b_2,b_3,...,b_K} + i|11...1\rangle_{1_1,b_2,b_3,...,b_K}\right]/\sqrt{2}$ is generated by half of the additional ancilla qubits and the first clock qubit of the central node. At the same time, the central node uses the other half of the additional ancilla qubits and each node to create a single Einstein Podolsky Rosen (EPR) pair. The central node performs k-1 independent Bell measurements on its additional ancilla qubit pairs. This transfers the qubit state to other clock nodes and measurement results are transmitted to each node through the classical channel. Each node makes unitary transformation accordingly to realize the quantum teleportation. The result of the transfer is a collective GHz state $\left[|00...0\rangle_{1_1,1_2,...1_K} + i|11...1\rangle_{1_1,1_2,...1_K}\right]/\sqrt{2}$, stretching across all K nodes. Finally, all nodes (including the centre node) extend the entanglement to all remaining clock qubits.

To extract the phase information of different GHz states after interrogation, each node measures its qubit on the x-basis and evaluates the parity of all measurement results. Then, the node sends the information to the central node through the classical channel. The central node calculates the total parity and extracts the phase information.

The measured value of the phase gives an estimate on the centre-of-mass (COM) detuning, which is subsequently used by the centre node to stabilize the COM laser signal. To this end, the centre generates the COM of the frequencies. Every node sends its local oscillator field to the centre via phase-stable optical links and the centre synthesizes the COM frequency by averaging the frequencies with equal weights. This can be implemented via the heterodyne beat of the local oscillator in the centre against each incoming laser signal resulting in K beat frequencies. Synthesizing these beat frequencies allows the local oscillator of the central node to phase track. The centre distributes the stabilized clock signal to different members of the network by sending individual error signals to all nodes, respectively, and corrects its own LO as well, accordingly. Alternatively, the centre can be operated to provide restricted feedback information to the nodes.

According to the theoretical analysis, the precision of the entangled quantum clock network is $\sqrt{K_n}$ times higher than that of the classical clock network under the same number of nodes and qubits, which breaks through the standard quantum limit and is closer to the Heisenberg limit.

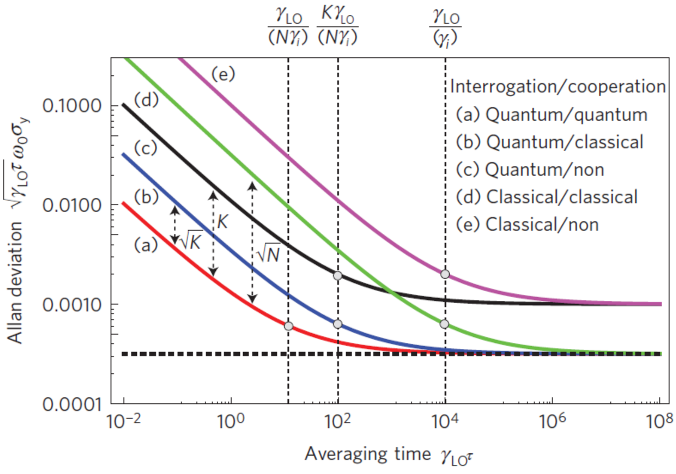


Figure 6 – Performance of different operation schemes

Attacks against this quantum clock network can be categorized as:

1) **Sabotage attacks:** These attacks describe a situation where one of the nodes intendedly or unintendedly operates in a damaging manner, e.g., one node could try sending false LO frequencies or wrong measurement bits in the hope of corrupting the collective measurement outcomes. To detect such malicious participants, the central node can occasionally perform assessment tests of the different nodes by teleporting an uncorrelated qubit state $\left[|0\rangle + e^{i\chi}|1\rangle\right]/\sqrt{2}$, where χ is a randomly chosen phase known only to the centre. By checking for statistical discrepancies between the measurement results and detuning of the LO signal sent by the node under scrutiny, the centre can rapidly and reliably determine whether a node is operating properly. This strategy, however, breaks down if multiple sabotage attacks happen in a short time.

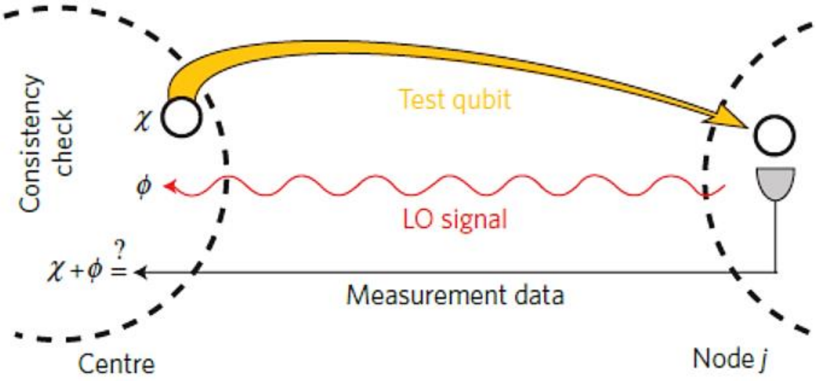


Figure 7 – Schematic of detecting sabotage

2) **Eavesdropping attacks:** Eavesdroppers may try to intercept the sent LO signals and synthesize the stabilized COM frequency ν_{COM} for themselves. However, this protocol minimizes the attainable information of this strategy by prescribing that only the non-stabilized LO signals are sent through classical channels. This requires the feedback to be applied to the LO signal after some of it has been split off by a beam splitter and the centre to integrate the generated feedback in time. Alternatively, eavesdroppers could try intercepting the LO and feedback signals to gain access to the same information the centre has. This can be prevented by encoding the radio frequency feedback signal with phase modulation according to a shared secret key. Since such a key can be shared securely with QKD, this protocol keeps the feedback signal hidden from outsiders. As a result, even if the hardest working eavesdropper (who intercepts all LO signals) were able to access the

non-stabilized COM signal, the stabilized COM signal remains accessible exclusively to parties involved in the collaboration.

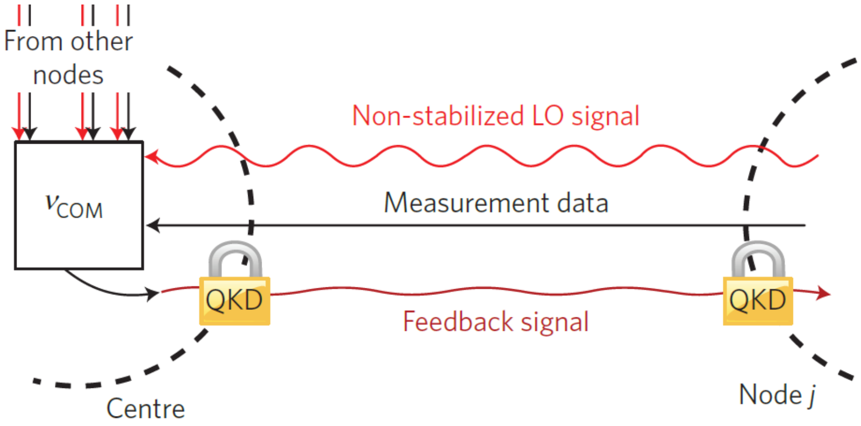


Figure 8 – Schematic of eavesdropping prevention

3) **Central node attacks:** Since the centre is the hub of all information, ensuring its security has the highest priority. In the case where the central node cannot be sufficiently trusted to play a permanent central role, a rotation scheme can be used. Changing the central node from time to time can greatly reduce the potential network vulnerabilities caused by an untrusted site. This requires a fully connected network and a global scheme for assigning central roles.

It is possible to achieve secure frequency synchronization in the quantum clock network (QCN) using the previously described defensive measures and through the above operation, frequency synchronization is realized among nodes in the quantum network, i.e., all nodes share a global standard oscillation frequency. To further realize time synchronization, i.e., to get the time difference between the local node and standard time source and calibrate it, it is necessary to run the point to multipoint (P2MP) quantum time synchronization protocol as illustrated in Figure 9.

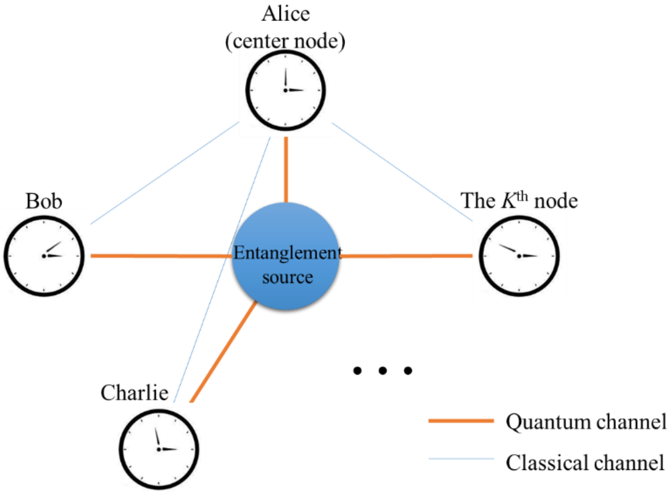


Figure 9 – Schematic of P2MP quantum time synchronization protocol

All *K* nodes in the quantum network share a *K*-qubits entanglement state. The simplest entanglement state is W-state, which is in the following form:

$$|\Psi(W)\rangle = \frac{1}{\sqrt{K}}\left(|100...00\rangle + |010...00\rangle + ... + |000...01\rangle\right) \tag{10}$$

The centre node, Alice, measures the qubit in her possession in the measurement basis |±>= (|0>±|1>)/√2 at standard time *t*=0 and broadcasts her measurement result to the other nodes via classical channels. The observers of the other clocks without synchronizing also measure their own qubits in the measurement basis at their own time t_i=0, which has a time difference Δ from the standard time.

For the case that the result measured by Alice is|+>, the others obtain the probabilities P with different outcomes:

$$P(|+\rangle) = \frac{K + 2\cos\omega\Delta}{2K} = \frac{1}{2} + \frac{\cos\omega\Delta}{K} \quad (11)$$

The time difference Δ between the network node's clock and standard time can be calculated by Equation (11). All the network nodes can correct their own clocks according to Δ_i, and then all the quantum network nodes realize time synchronization.

6.1.3.5 Application prospects

A quantum network of clocks can have important scientific, technological and social implications. Besides creating a worldwide platform for time and frequency metrology, such a network may find important applications in other areas such as earth science, precise navigation of autonomous vehicles and space probes (requiring high refresh rate) and the testing of and search for fundamental laws of nature, including relativity and the connection between quantum and gravitational physics.

However, UC-QTS-003 is currently at an experimental research stage and does not meet conditions for commercialization.

6.2 Quantum computing use cases

The quantum computing use cases described in this report are focused on the application and method of quantum computing, each with different requirements and features as shown in Table 2.

Table 2 – Features of different use cases for quantum computing

ID	Name	Features
UC-QC-001	Quantum cloud computing	User data, code, resources, etc. are fully hosted in the cloud computing platform.
UC-QC-002	Distributed quantum computing	In the distributed quantum computing network, the quantum chipsets realize the expansion of computing power in the form of tensor product in the entangled state
UC-QC-003	Blind quantum computing	Quantum/classical client and quantum server adopt the security enhancement technology of quantum cryptographic protocol
UC-QC-004	Quantum simulator in centralized/distributed quantum computing	Within the data centre or across the WAN networking scenario, the classical computing server cluster performs meaningful quantum computing circuit simulation tasks
UC-QC-005	Hybrid classical and quantum computing	The classical and quantum computing units cooperate and work together via classical communication networks.

6.2.1 UC-QC-001: Quantum cloud computing

6.2.1.1 Use case description

Potential applications of UC-QC-001 range from basic research to commercial use such as big-data processing, artificial intelligence (AI), material design, and traffic flow optimization. One well-known application of quantum cloud computing is variation quantum Eigen (VQE) solver-based quantum chemistry simulations where a classical computing server (cloud) is iteratively used to adjust control parameters of a quantum chip to find the energy spectrum of a given chemical structure. The result of the VQE simulation can be used for medicine design, oil processing and so on.

Target end users for UC-QC-001 include researchers, students, governmental organizations, and private companies interested in the study and use of quantum computing techniques for research, education, and industry applications.

6.2.1.2 Problem statement

Resources required for quantum computing may be beyond what an end user can afford. The question is thus: *Is there a solution that gives access to quantum computation technology to as many end users as possible at an affordable cost per end user?*

6.2.1.3 Motivation/advancement

The amount of data today's society processes per day continues to grow exponentially. The electronic circuit line width of silicon-based computer chips has been narrowed down to nearly the atomic scale where quantum effects take over. It is well-known that in the atomic domain, quantum computing techniques show exponential speedup or use significantly less resources than classical computers to solve some difficult problems such as factorizing a big number into primes. However, the manufacturing techniques to produce a quantum computer are not mature yet and may be too expensive to allow an individual or small organization to exclusively own one. The solution presented in clause 6.2.1.4 and Figure 10 brings the benefits of quantum technology to many end users while remaining at low cost per user.

6.2.1.4 Technical solution

Quantum cloud computing (QCC) is a commercial model that allows many users to run quantum computing programs at an affordable price per user, see Figure 10. In a QCC system, a simulator and/or real quantum computing hardware is settled in a centralized server/hub, as called cloud, and the remote end users (or classical client) can access it via traditional internet/network or perhaps the quantum internet/network in the future. Presently, the technologies of the classical network and computing, such as the quantum simulator and software in cloud platform, are ready to support QCC solutions.

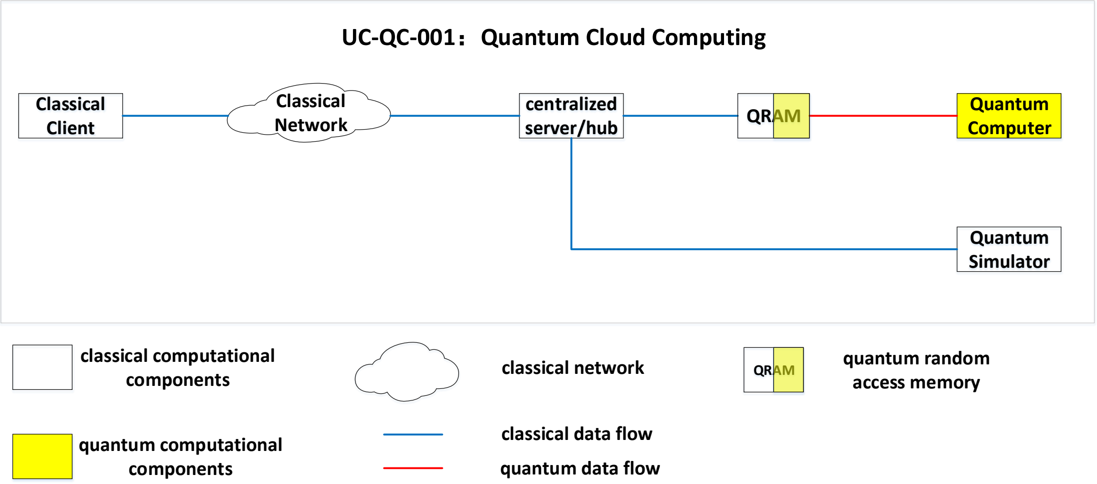


Figure 10 – Networking and computation model of quantum cloud computing

6.2.1.5 Application prospects

Quantum computing is usually described in a quantum circuit model with N qubits, which can be spanned into a $2^N \times 2^N$ matrix space mathematically. Due to the nature of quantum computing, a user would have to load a great amount of data if they wanted to read out an N-qubit quantum system faithfully. Petabyte order of magnitude of classical bit data has been generated when simulating a 45-qubit quantum circuit [b-Häner]. Of course, in a real physical quantum circuit or by using some tricks, readable data can be sampled by measuring some quantum observables and this process might reduce the amount of classical data to be transferred to an end user. However, it will still yield a great pressure of load to the classical network when the number of qubits is large. As the simulators and physical chips of quantum computers scale up, current networks will need to be upgraded in all aspects for the quantum computing service to be hosted over a communication network. New types of networks are even required to be built if the output of data is transferred over a pure quantum internet.

The QCC service, either deployed using simulators or quantum hardware, has emerged and is providing free or low-cost computing experience to a broad range of end users in the frontier of quantum studies. In the foreseeable future, it could bring revolutionary and cost-efficient computational capability to a broad spectrum of applications including in civil administration, medicine development, material industry, environmental preservation, etc. In comparison to alternative technologies, QCC is believed to have the best performance-to-cost ratio as different users keep using the machine without owning it.

6.2.2 UC-QC-002: Distributed quantum computing

6.2.2.1 Use case description

Similar to UC-QC-001, UC-QC-002 also employs quantum computing technologies based on a distributed network of quantum devices to run quantum algorithms. Its applications cover both basic research and commercial uses like big-data processing, artificial intelligence, material design, and optimization of complex systems, etc.

Target end users for UC-QC-002 include quantum device owners, researchers, students, governmental organizations and companies interested in the study and use of quantum computing techniques for research, education, and commercial applications.

6.2.2.2 Problem statement

A quantum computing chip is very difficult to scale up while remaining at good fidelity. This is due to the growing coupled noise in the chip and with the environment when the system expands. However, there are many small-scale quantum devices distributed in various labs. The question, thus, is: *Is it possible to build a network of distributed quantum hardware to lift the computational power beyond any single quantum chip has?*

6.2.2.3 Motivation/advancement

A quantum chip's computational power is limited by the number of qubits and the topological complexity of the chip. It is predicted that connecting different quantum chips into a network may yield a computational power greater than the direct sum of the computational power that individual chips have.

6.2.2.4 Technical solution

Distributed quantum computing (DQC) is a technology based on networks of distributed quantum chips that allow computational power multiplications of individual quantum devices, see Figure 11. In a DQC system, the tensor-product-like coupling of the joint quantum computing network generates computational advantages over the sum of individual chips' capability. Presently, technologies of quantum computational components and quantum networks require further study, therefore this solution is still in very early stages of development.

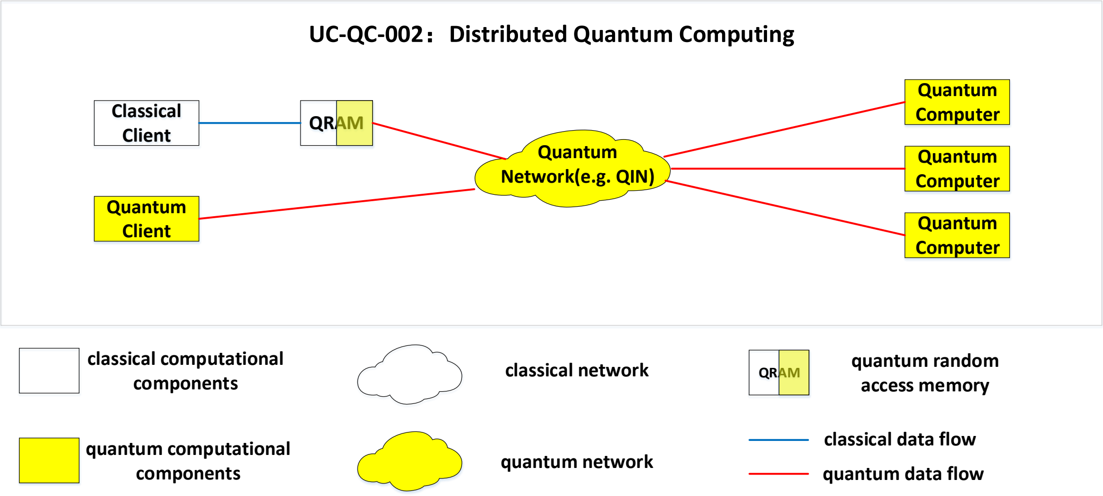

UC-QC-002：Distributed Quantum Computing
Classical Client
QRAM
Quantum Client
Quantum Network(e.g. QIN)
Quantum Computer
Quantum Computer
Quantum Computer
classical computational components
quantum computational components
classical network
quantum network
QRAM
quantum random access memory
classical data flow
quantum data flow

Figure 11 – Networking and computation model of distributed quantum computing

6.2.2.5 Application prospects

As shown in Figure 12, one of the most promising quantum algorithms that can run on near-term intermediate scale quantum (NISQ) computing hardware is variation quantum algorithm (VQA). VQA can be adapted to quantum chemistry applications through variation quantum eigen solver (VQE) and optimization applications through quantum approximate optimization algorithm (QAOA). Both algorithms can be realized using a DQC system by encoding the original problems with compound Hamiltonian terms. Taking the QAOA case, for instance, a full QAOA quantum circuit can be decomposed into many smaller sub-circuits which can be scheduled and executed on individual nodes of a DQC system. Then, the expectation value of an observable of the whole system can be calculated on a classical computer (the master node) by collecting measurement results of individual nodes with a given set of control parameters for distributed sub-circuits. To find a solution of the corresponding quantum chemistry problem or the combinatorial optimization problem, one iteratively calculates the expectation value by updating the set of control parameters until convergence.

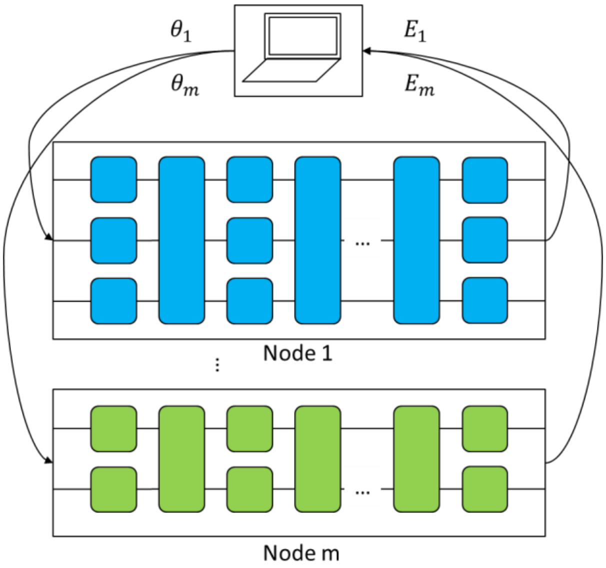


Figure 12 – An application of quantum computing on distributed networks

A DQC system is expected to be implemented over classical and/or quantum networks to enhance the computational power beyond any single unit's capability in the network. In the foreseeable future, it may bring revolutionary and cost-efficient computational capability to a broad spectrum of applications including in civil administration, medicine development, material industry, environmental preservation, etc. It may also solve the scale-up problem that limits individual chips.

6.2.3 UC-QC-003: Blind quantum computing

6.2.3.1 Use case description

Focusing on enhancement of security and authorization schemes for computation and data when running quantum computing over networks, the applications of blind quantum computing cover both basic research and commercial uses like big-data processing, artificial intelligence, material design, and optimization of complex systems, etc.

Target end users for UC-QC-003 include quantum device owners, researchers, students, governmental organizations and companies interested in the study and use of quantum computing techniques for research, education, and commercial applications.

6.2.3.2 Problem statement

Quantum computation shows great potential for solving some important problems faster than classical computation. However, a practical quantum computer needs to be large enough to handle sufficient numbers of delicate qubits, perhaps extending into the high millions or low billions of physical qubits. Large-scale quantum "mainframes" will be valuable resources and time-sharing of machines will be economically attractive. Time-sharing quantum cloud services will allow owners of smaller quantum computers to perform large quantum computations. Sometimes the input and output data are private and even the choice of quantum computing algorithms may be sensitive information, so they have to be kept secret even from the server [b-Morimae-1]. The question thus is: "*Is there a technical solution within quantum aspect that can let the client execute quantum computations on a server without revealing any secret information about the computation?*"

6.2.3.3 Motivation/advancement

In recent years, several protocols have emerged which seek to tackle the privacy issues raised by delegated quantum computation. Going under the broad heading of blind quantum computing (BQC) provides a way for a client to execute a quantum computation using one or more remote quantum servers while keeping the structure of the computation hidden. While the goal of BQC protocols is to ensure the privacy of the computation, many of them also allow for verification of the computation being performed by embedding hidden tests within the computation.

6.2.3.4 Technical solution

As shown in Figure 13, BQC is a technology that combines notions of quantum cryptography protocols [b-Morimae-1], [b-Morimae-2], [b-Sheng], [b-Li] and quantum computation. It can fulfil quantum computation by a client with limited or even no quantum computational power with the help of an unreliable quantum server while keeping the privacy of the client's algorithm and the data. Today's BQC technical solutions, computation and networking protocols are quite active, but it may take a relatively long time to realize BQC in engineering.

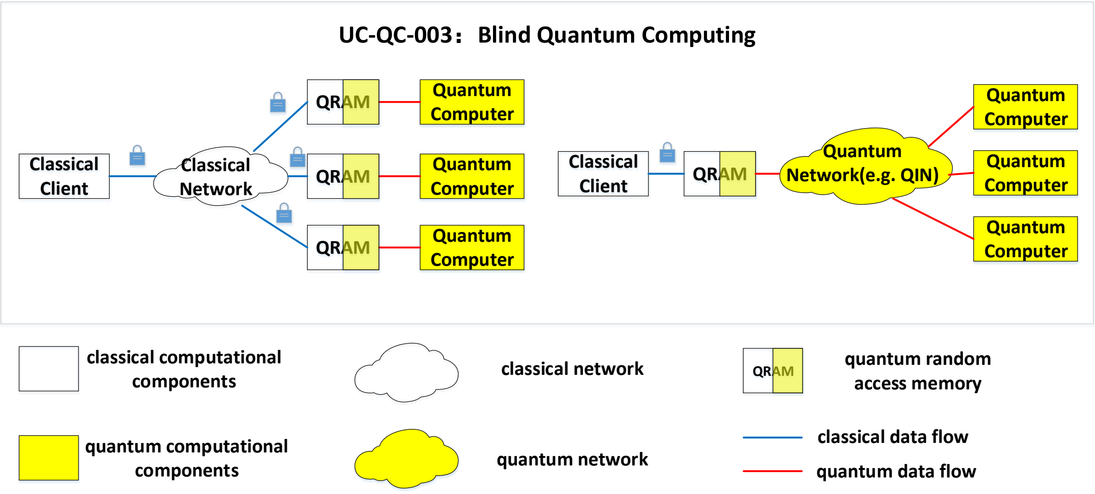


Figure 13 – Networking and computation model of blind quantum computing

6.2.3.5 Application prospects

A BQC system is expected to be implemented over classical and/or quantum networks to enhance the security and authorization scheme for computation and data through the network. In the foreseeable future, it may bring revolutionary capability to these applications which are sensitive in data security and personal privacy including e-commerce, finance, banking, insurance, medical treatment, etc.

6.2.4 UC-QC-004: Quantum simulator in centralized/distributed quantum computing

6.2.4.1 Use case description

Recent technical advances have brought the world closer to realizing practical quantum (circuit) simulators: engineered quantum many-particle systems that can controllably simulate complex quantum phenomena. Quantum simulators can address questions across many domains of physics and scales of nature, from the behaviour of solid-state materials and devices, chemical and biochemical reaction dynamics, to the extreme conditions of particle physics and cosmology that cannot otherwise be readily probed in terrestrial laboratories.

Target end users for UC-QC-004 include quantum device owners, researchers, students, governmental organizations, and companies interested in the study and use of quantum computing techniques for research, education, and commercial applications.

6.2.4.2 Problem statement

Quantum simulators are a promising technology on the spectrum of quantum devices from specialized quantum experiments to universal quantum computers. These quantum devices utilize entanglement and many particle behaviours to explore and solve hard scientific, engineering, and computational problems. Rapid development over the last two decades has produced more than 300 quantum simulators in operation worldwide using a wide variety of experimental platforms [b-Altman]. Recent advances in several physical architectures promise a golden age of quantum simulators ranging from highly optimized special purpose simulators to flexible programmable devices. These developments have enabled a convergence of ideas drawn from fundamental physics, computer science, and device engineering. They have strong potential to address problems of societal importance, ranging from understanding vital chemical processes, enabling the design of new materials with enhanced performance, to solving complex computational problems. In practice, a hybrid system may be helpful to improve the precision of quantum simulators, where a classical computer server is applied to help optimize parameters of quantum simulators based on optimal quantum control technique or feedback/feed-forward mechanism.

Beside the quantum simulation using quantum devices, equivalent quantum circuit models can be derived and simulated on a classical computer or a cluster of classical computers. This type of simulator is called a quantum circuit simulator and they are crucial before quantum devices become mature enough and robust to noise. Currently, quantum circuit simulators are also useful tools to verify quantum computing algorithms and to develop quantum software. Since it usually requires a large scale of clusters to run a meaningful circuit simulation, a quantum circuit simulator is usually deployed on a cloud server.

In many cases, large scale quantum computation tasks with quantum (circuit) simulators may relay on distributed computing clusters over cloud environments in which clients and servers may be in local or wide area networks.

6.2.4.3 Motivation/advancement

Centralized or distributed quantum computing applications enabled by classical communication networks have many forms. Taking currently available commercial models as an example, quantum circuit simulators on cloud, control pulse optimization service, and classical-quantum hybrid computing service are well-known instances of these forms. However, existing networks are not specifically designed for these quantum computing applications. There are still challenges and requirements for the existing classical communication networks such as big data traffic and communication overheads, deterministic delay and/or low-latency, high security and privacy, reliability or robustness, etc.

These services require massive computing power which could be implemented by centralized or distributed classical computation over classical networks that may not exist for a long time. Three typical network components for a general quantum computation service over classical networks, as illustrated in Figure 14, are:

– **Component Class A (inner network):** Interconnection and communication networks of computation clusters merely inside a Data Center (DC).

– **Component Class B (edge network):** Key networks components linking different DCs in a local network.

– **Component Class C (wide network):** Key network components linking different DCs yet across a wide area network.

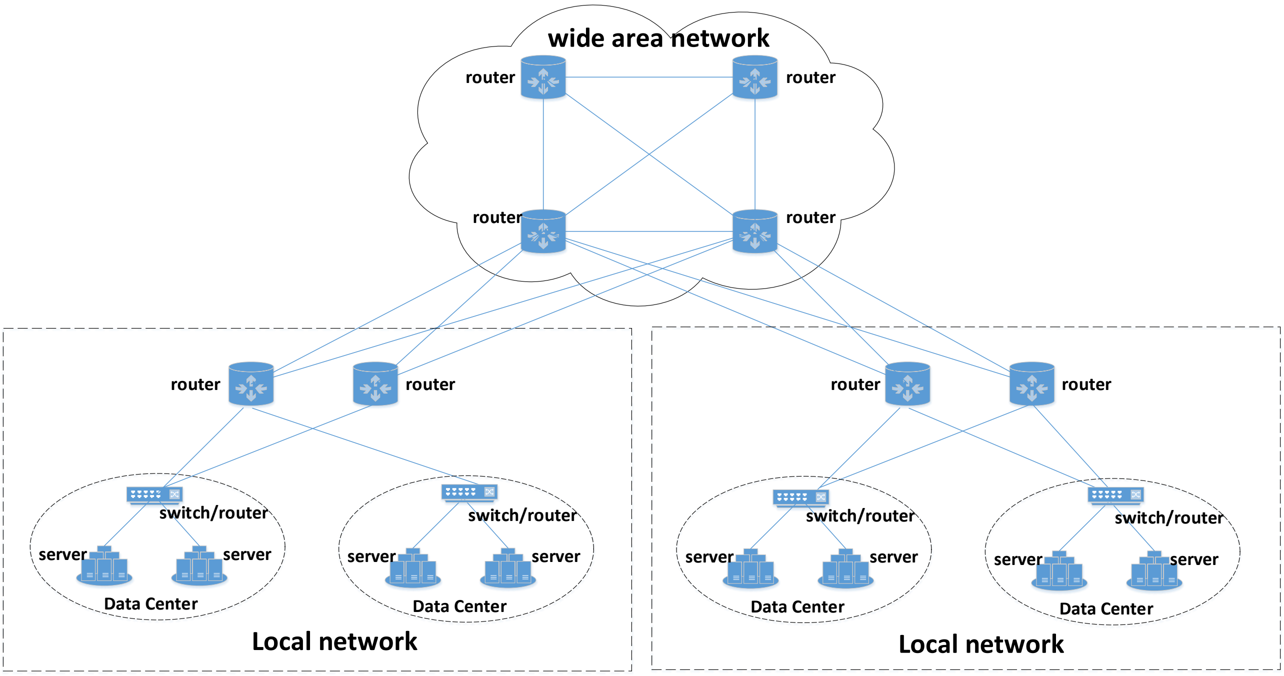


Figure 14 – Typical network scenario of computation clusters over classical networks

It should be noted that different network component classes have different network environments (such as physical topology, bandwidth, delay, bit error rate, node/link stability, packet loss rate), which may adopt different computation/communication architectures (such as parameter servers and all-Reduce), parallel modes (such as data parallel and model parallel), and communication methods (such as synchronous communication and asynchronous communication) to form different computation-communication frameworks. Different frameworks have different transmission modes (such as the logical topology of parameter synchronization), communication overhead and communication pace and other traffic characteristics, which have different degrees of impact on synchronization time and system scalability.

However, existing networks are not fully prepared for these quantum computing applications. There are still some challenging requirements for suitable classical communication networks as described below:

– **Reducing big data traffic and communication overhead:** considering the high capacity and communication of quantum computing, these use cases of QIT over traditional networks may generate considerable amounts of data over the internet and could greatly impact current network infrastructure. [b-Häner] reports that a scheduling algorithm was applied to quantum supremacy circuits in order to reduce the required communication and simulate a 45-qubit circuit on the Cori II super-computer using 8192 nodes and 0.5 petabytes of memory. A large amount of computing performance was used to handle the communication load while the communication load could still account for 75% of the calculation time.

– **Deterministic delay and/or low-latency:** some applications such as running some VQE and QAOA instances rely on feedback between classical and quantum components to update the state of computation which may need timely information exchange across wide areas of a network. In addition, quantum machine learning (QML) usually requires multiple iterations of gradient model parameter updates. Bad performance of delay would reduce the efficiency of model convergence and even lead to failure of QML training.

– **High security and privacy:** the security of computation and communication between different nodes in classical networks is essential and, for data-sensitive applications in particular, data privacy and user authentication is even more essential.

– **Reliability or robustness:** the reliability or robustness of a network should be guaranteed during the life cycle of computation tasks and data exchange in distributed quantum computing enabled by classical communication networks. However, this may not be fully satisfied with the TCP/UDP protocols of the current best effort design of the internet.

There are, however, some novel techniques induced by new service requirements over classical networks, for example content delivery networks (CDNs) were designed to improve the performance of real-time video streams, IEEE 802.1 time sensitive network (TSN) was proposed and standardized for low latency and rapid response demand of industrial internet etc.

Existing classical networks are required to either be adapted, adjusted or re-designed to serve these quantum computing applications and novel services.

6.2.4.4 Technical solution

The technologies of a quantum simulator in centralized/distributed quantum computing are completely implemented within the framework of classical networks and classical computation which can serve as a relatively mature solution at present, see Figure 15. It is noted that quantum computing tasks done using a quantum simulator can be regarded as a new service supported by classical network and classical computing.

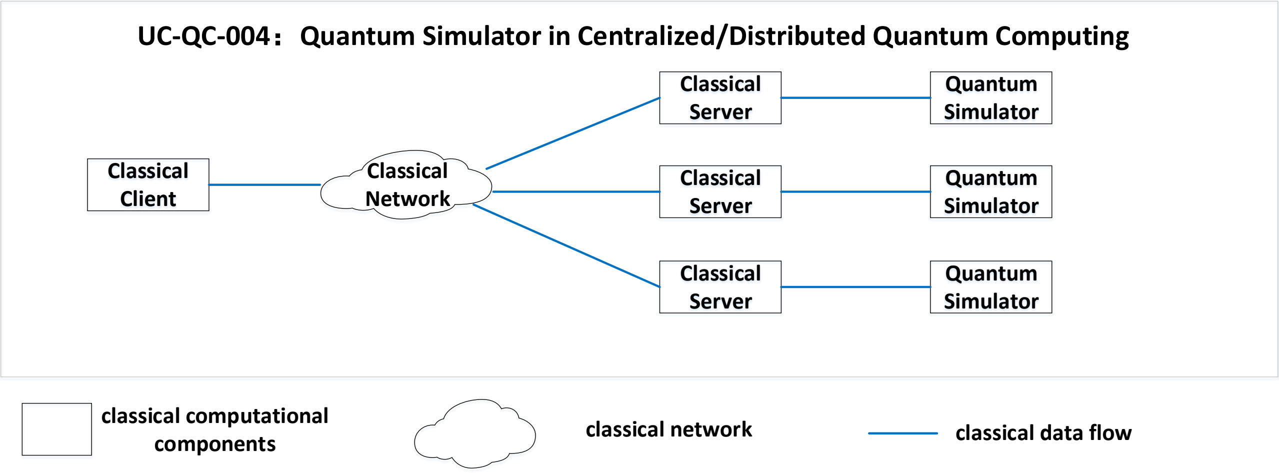


Figure 15 – Networking and computation model of quantum simulator in centralized/distributed quantum computing

However, distributed quantum computing tasks executed on quantum (circuit) simulators over classical networks still face some technical challenges. Potential quantum-computing-motivated technical solutions such as blockchain, RDMA, lightweight cryptography, self-adaptive and intelligent routing schemes as well as resource scheduling mechanisms, etc. are proposed for further discussion:

– To fulfil the reduction of big data traffic and communication overhead, highly-tuned kernels [b-Häner] in combination with novel parallel acceleration and reusing technologies are considered for further studies, including extraction and optimization of communication load characteristics under specific QC services, novel parallel collaboration policy of models, computation and communication architectures, novel logical networking schemes different from traditional fat-tree architecture, novel networking protocols different from TCP/UDP etc.

– To fulfil the low-latency feature of networks for these use cases, one might want to consider remote direct memory access (RDMA) technology as shown in Figure 16. Compared to the classical TCP/IP network, RDMA can directly access the memory of another machine from one machine without any processing of the target machine's operating system. Direct memory access avoids copying data twice from the user mode to core mode and back to user mode, saving the CPU occupancy of the target machine and effectively improving throughput and reducing latency. The flow control technology (namely PFC) used on the switch side of the RDMA network can avoid packet loss caused by buffer overflow in the switch thereby eliminating the in-cast phenomenon.

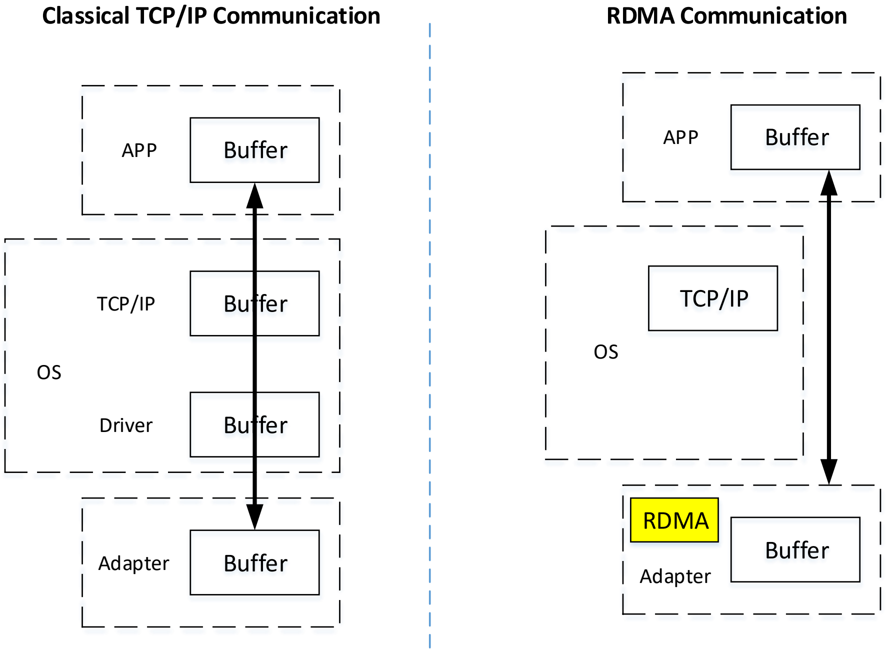


Figure 16 – Classical TCP/IP communication vs RDMA communication

For some cases, a determined response latency is crucial for quantum control and some hybrid computing scenarios which may require a self-adapted resource allocation protocol for networking. Furthermore, self-adaptive and intelligent routing schemes and resource scheduling mechanisms are also worth studying to adapt the characteristics of simulated quantum computing and unique service traffic distribution over classical networks to balance local computation and communication over networks. In Figure 17, considering the special characteristics of QC data distribution vs latency over network with a long-tail, a QC-aware device or module can be designed to reshape the probability density function (PDF) of QC data flow vs latency under self-adaptive and intelligent routing scheme and resource scheduling mechanism to control end-to-end delay/latency of specific QC tasks on demand.

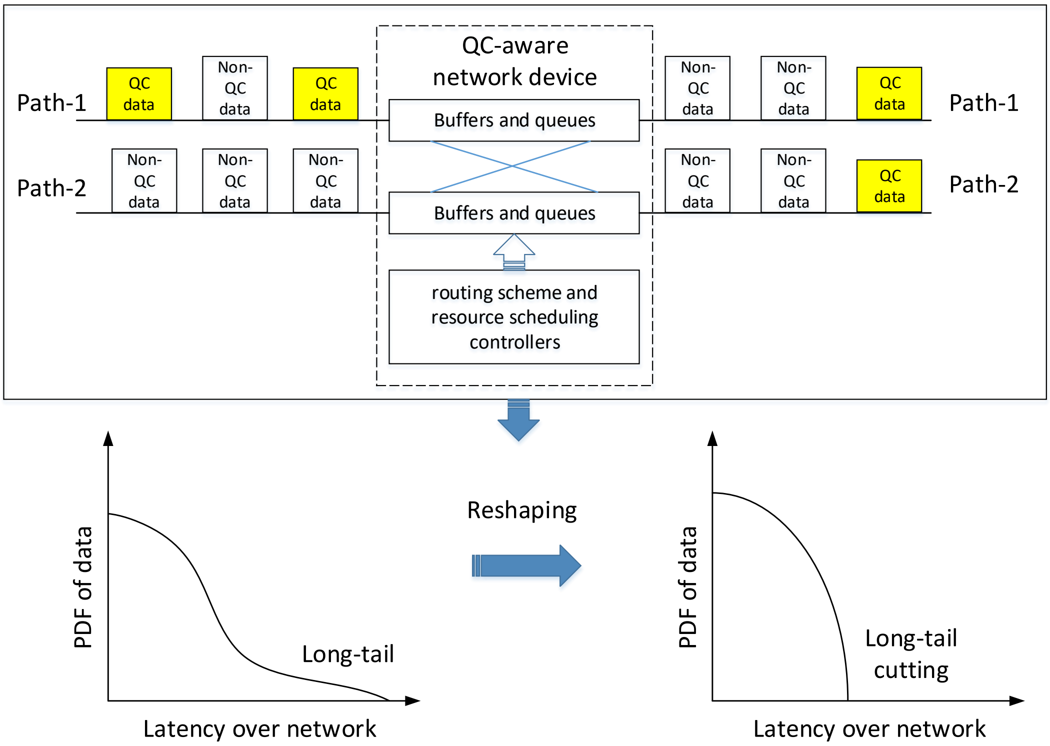


Figure 17 – Latency control over network towards simulated Quantum computing (QC) service

– To fulfil the security and privacy requirements of quantum computing applications over classical networks, new lightweight cryptography technologies are required. Otherwise, the encoding process of cryptography over the large amount of data will inevitably increase the time delay and communication overhead from end to end. Hardware-based cryptographic methods may be helpful for this purpose. Blockchain may also be useful for tracking data flow.

– To fulfil the reliability or robustness of networks while a great amount of data is transferring, high-efficient lossless data transferring technologies should be studied. Naturally, how the channel capacity affects the computational precision of quantum computing scenarios relying on the feedback between classical and quantum components (like some VQE and QAOA algorithms etc.) may be a good direction to pursue. For some quantum computing tasks under NISQ, whether the final calculation performance can allow packet loss over complex and large-scaled networks and tolerate some transmission errors is also a new direction worth studying. In addition, based on the characteristics of quantum simulation computing and unique data distribution, a quantum computing-aware routing and protection strategy should be adopted to design an intelligent logical topology over physical topology of networks.

In summary, descriptions and analysis of QC service, network challenges and potential QC motivated technical solutions are shown in Table 3.

Table 3 – Descriptions and relationship of QC service, network challenges and potential QC-motivated technical solutions

Challenges and requirements of classical networks	Service of QC by simulators	Potential quantum computing motivated technical solutions
Reducing big data traffic and communication overhead	Full amplitude QC with large qubits, etc.	Highly tuned kernels in combination [b-Ebubechukwu], novel parallel collaboration policy, novel logical networking scheme, novel networking protocol etc.
Deterministic delay and/or low latency	VQE, QAOA, QML, etc.	RDMA, self-adaptive and intelligent routing scheme and resource scheduling mechanism, TSN techniques in IEEE 802.1 AS etc.
High security and privacy	2B service of QC, e.g., Finance, Medical, Aerospace etc.	Blockchain [b-Giovannetti-3], Differential Privacy (DP) [b-Hong], Homomorphic Encryption (HE) [b-Valencia], Federated Learning (FL) [b-Xie] etc.
Reliability or robustness	2C service of QC, QC over scenario C (wide network), etc	high-efficient lossless data transferring technologies, quantum computing-aware routing and protection strategy etc.

6.2.4.5 Application prospects

Emerging quantum (circuit) simulators over classical networks will support creative, cutting-edge research in science and engineering to uncover new paradigms, advance nascent hardware platforms and develop new algorithms and applications for a new generation of quantum simulators. This effort will further support the development of new materials and devices to help accelerate the progress of new technologies and push them out of the research laboratory.

6.2.5 UC-QC-005: Hybrid classical and quantum computing

6.2.5.1 Use case description

QAOA is a variational based quantum-classical hybrid algorithm to solve combinatorial optimization problems in near-term gate-based noisy intermediate-scale quantum computer. The original form of QAOA aims at finding the ground states of some special Hamiltonian which encode the solutions of specifying combinatorial optimization problems such as Max-Cut problem, satisfiability problems (SAT). More recently, QAOA is developed as the quantum alternating operator ansatz which can also be useful for tackling those problems with some constraints such as the max independent set, travelling salesperson problem. In addition, QAOA is also found to be helpful for solving the problems of linear equations and factoring problem.

Recently there have been some demos of the application of VQE, for example, the first experiment in photonic quantum processor [b-Peruzzo], the experiment to simulate larger systems [b-Kandala-1] and the chemical reaction [b-Arute]. There are also other methods that can be developed based on VQE, such as QAOA and QML. These methods can be used to solve different types of eigenvalue problems which are useful in science and common life.

Target end users for UC-QC-005 include quantum device owners, researchers, students, governmental organizations and companies interested in the study and use of quantum computing techniques for research, education, and commercial applications.

6.2.5.2 Problem statement

There are some typical computation problems which may run on classical quantum hybrid computing architecture such as quantum approximate optimization algorithm (QAOA) and variational quantum eigensolver (VQE).

6.2.5.2.1 QAOA problem

Combinatorial optimization problem is a subfield of mathematical optimization. It has important applications in several fields in the real world, including reducing the cost of supply chains, vehicle routing, job allocation and so on. Generally speaking, the task of combinatorial optimization is to find the object that minimizes the cost function from a limited number of objects.

QAOA is a variational quantum algorithm that promises to solve combinatorial optimization problems by a parameterized quantum circuit. It also has potential to solve linear equations and realize quantum machine learning. In a QAOA implementation, the expectation value of the objective Hamiltonian given by the parameterized circuit represents the objective function of the combinatorial problem and the goal of QAOA is to minimize this objective function via a classical optimizer. Classical computers can also play more roles in QAOA, such as recursive QAOA, adaptive QAOA, and optimizing parameters by machine learning, these approaches are expected to further improve the performance of the algorithm.

As a heuristic algorithm the advantages of QAOA are still uncertain. Therefore, the algorithm performance research on large-scale problems may need to rely on distributed computing clusters over cloud environment.

6.2.5.2.2 VQE problem

One of the most important problems in science is the eigenvalue problem. For instance, if the ground state and corresponding energy are known in a molecular system, many useful properties can be derived to analyze the system since molecular systems are usually in the ground state. To calculate the ground state, many methods have been developed. However, for large systems over tens of electrons, these methods need so many computation resources that even the best supercomputer cannot give a result with enough accuracy.

Since quantum computation is developing fast these years, scientists are attempting to make use of quantum computers to simulate molecular systems and calculate the ground state energy. The VQE algorithm, which was recently proposed as a method to calculate the ground state energy of molecules, is a method believed to have exponential acceleration compared to classical methods and is believed suitable for the NISQ era.

There is a lot of research related to the development of VQE focusing on resolving these important problems: "*What is the most practical way to run the algorithm on real quantum hardware?*" and "*What problems can be solved by VQE efficiently recently?*".

6.2.5.3 Motivation/advancement

One of the most significant problems in quantum computing is how to demonstrate quantum supremacy. It is particularly important to achieve this goal by using existing quantum resources, i.e., the noisy intermediate scale quantum computer (NISQ). On the other hand, the combinatorial optimization problems have lots of applications, but most of them are NP hard problems. As the scale increases, finding their solutions will be beyond the ability of the classical computer and although adiabatic quantum algorithms have been proposed to tackle such problems, it is not on NISQ algorithm. The variational gate-based quantum-classical hybrid algorithm (one of which is the QAOA) is the most promising method to demonstrate quantum supremacy on NISQ.

VQE has been tested in many experiments. Since present quantum hardware is not powerful enough to run VQE algorithm for large systems, it is important to make different adjustments based on the hardware condition. For example, the error in the quantum hardware is not negligible which requires practical error mitigation methods and the coherent time in the quantum hardware is currently short, thus needing careful design of the circuit structure.

6.2.5.4 Technical solution

In the framework of hybrid classical and quantum computing, as shown in Figure 18, the technologies of the classical part related to computation and networking are relatively mature whereas for the quantum computing part such as QRAM and quantum computer, further development is either still ongoing or have not yet been adopted at a large scale for application.

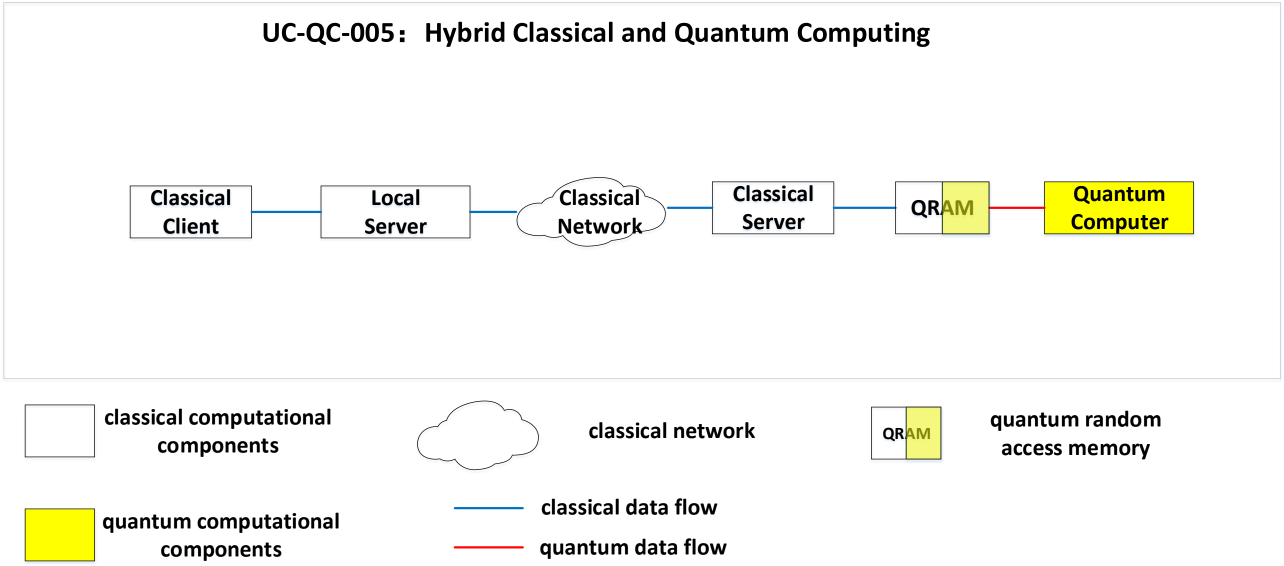

UC-QC-005：Hybrid Classical and Quantum Computing
Classical Client
Local Server
Classical Network
Classical Server
QRAM
Quantum Computer
classical computational components
classical network
QRAM
quantum random access memory
quantum computational components
classical data flow
quantum data flow

Figure 18 – Networking and computation model of hybrid classical and quantum computing

As for the algorithm and software parts, the VQE algorithm is based on the variation method. Basic steps of VQE include qubit encoding, mapping the operators, ansatz preparation, together with several techniques for improving the performance, including constraining, and error mitigation. There are many efforts dedicated towards improving the performance of VQE and some technical solutions include designing different ansatz for specific problems and hardware [b-Kandala-1], [b-Arute] and developing methods to deal with errors [b-Kandala-2].

Nowadays there are some applications of classical and quantum hybrid computing over classical communication networks which can be summarized into two types:

– **Type I**: user accessing the internet, pre-processing data in the local client and uploading the data and computing job to a remote quantum computing device which may pass through a wide area network. Typical applications are some QC services such as quantum annealing (QA) where classical computation is responsible for data processing in the user's local computer while quantum computation is designed for solving combinatorial optimization problems.

– **Type II**: distributed classical and quantum hybrid computing applications over local/wide area classical networks. e.g., algorithm applications such as VQE, QAOA, QML etc. working under schemes of classical training/measured/controlled data's feedback which needs classical and quantum computation working together.

In this report, some results analysis is provided aiming at two aspects, i.e., network latency and data reliability which may impact the quality of service utilizing classical and quantum hybrid computing over classical communication network.

6.2.5.4.1 Type I application related to network latency and data reliability

Taking the example illustrated in Figure 19 where users develop a traffic optimization application, some requirements for the Type I application are listed below:

- The system contains such essential software components as Component-1 (data import and demand mapping), Component-2 (solving combinatorial optimization problem) and Component-3 (visualization of results analysis)
- Users would expect to develop Component-2 under the service provided by real quantum computation infrastructure such as a QA device via the internet because of its computational advantage aiming to solve this problem for traffic optimization
- With consideration for software property rights and service protection, Component-1 and Component-3 are not allowed to be uploaded but are ran on a cloud platform

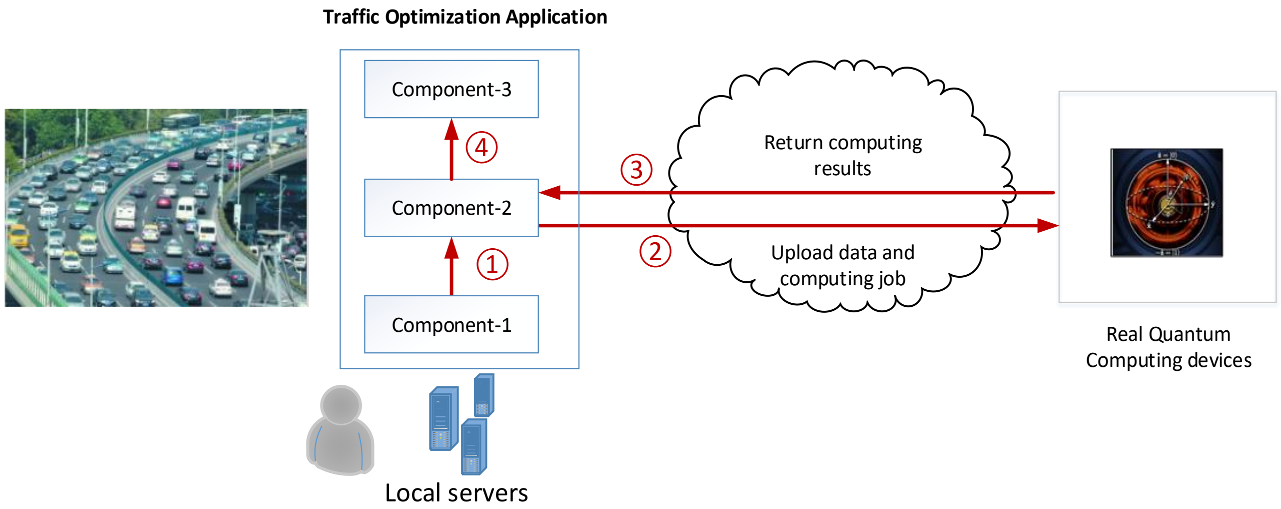

Traffic Optimization Application
Component-3
④
Component-2
①
Component-1
③
Return computing results
②
Upload data and computing job
Real Quantum Computing devices
Local servers

Figure 19 – Type I application over classical networks

Based on the analysis above, it is clear that the quantum computation in Component-2 and classical computation in Component-1 and Component-3 should work together to provide an integral service for the traffic optimization application.

As illustrated in Figure 19, datasets are pre-processed in the user's local computer and uploaded to the server or platform equipped with real quantum computing devices, then computing results are returned to users over classical networks. For example, when designing a QA algorithm to solve the optimization and combination problem, data may first be formulated as quadratic unconstrained binary optimization (QUBO) or Ising model with some classical operation and then the model uploaded to the remote real quantum device to finish the QA process. It is noted that this application requires only one ping-pong communication over classical networks.

The impact analysis of the QC service with respect to network latency and data reliability is thus:

- **Impact of network latency for QC service:** The uploaded data, computation job and returned results may transfer over a wide area network thus the user may have to wait for long time to receive the results and have difficulty estimating the completion time for the whole process. Although the execution speed of quantum computing is very fast, the long delay leads to a decline in competitiveness with classical computing.
- **Impact of data reliability for QC service:** Data loss is likely to cause the failure of quantum computing tasks, especially in the case of large amounts of dataset uploading, which seriously affects the user experience. In this case, huge amounts of burst data may pour into wide area networks which bring great challenges to networking technology such as flow control, routing, scheduling etc. to guarantee low or determinate latency and big data reliability.

6.2.5.4.2 Type II application related to network latency and data reliability

Some machine learning (ML) applications are sensitive to users' data and as illustrated in Figure 20, federated machine learning (FML) introduced in [b-IEEE P3652.1] shows a distributed computation framework where data from different owners is prohibited to move out of local nodes so that the ML model is trained or inferred across classical networks to make a double-win for data privacy and ML implementation.

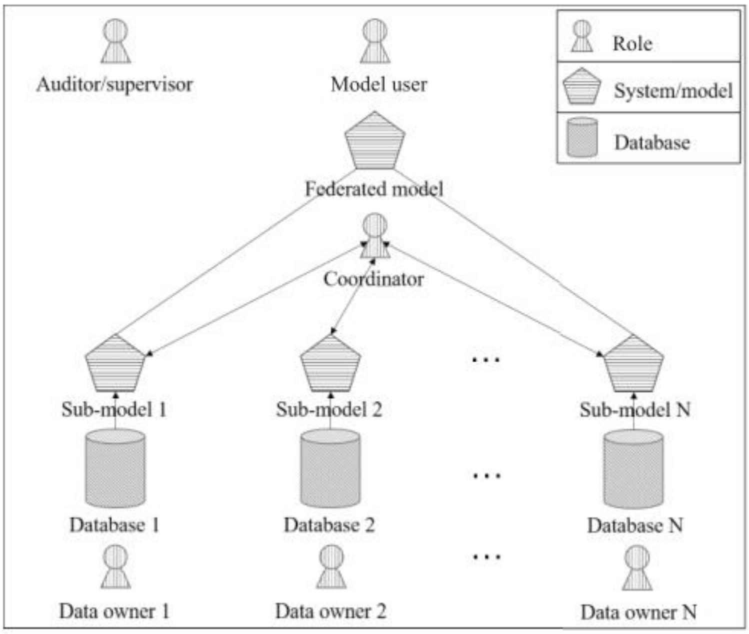
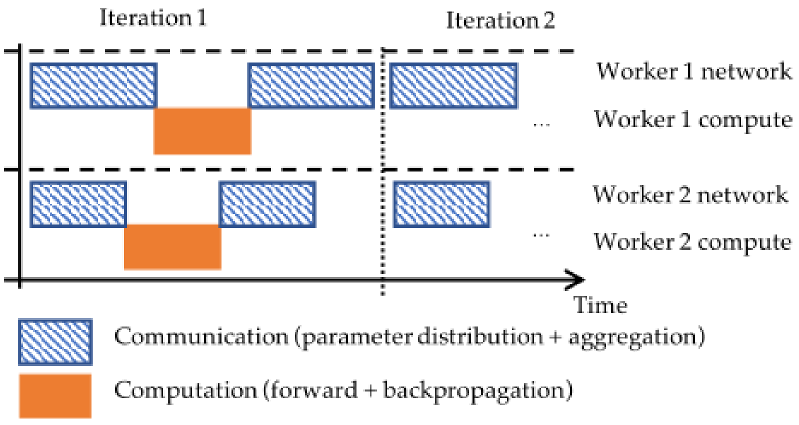


Figure 20 – A schematic diagram of FML framework introduced in [b-IEEE P3652.1]

One consideration for introducing quantum computation in FML is that encryption and decryption of the ML model and data unavoidably brings a huge computational overhead. For example, holomorphic encryption (HE) employed in FML produces at least 100 times more computation than original distributed machine learning (DML). Quantum computation can accelerate the speed of computation for encryption and decryption during the pipeline of FML. The hybrid computation solution can promote the quality of service for DML/FML.

Taking the example of DML applications, synchronized distributed training is often used to handle huge datasets. In the distributed training process, multiple worker nodes train the same model. In each iteration, workers fetch the current parameters of the models, train the model locally and exchange their results to update a global model, as Figure 21 shows.



NOTE: **Common pattern of distributed ML jobs. Workers need to wait for other workers to finish the current iteration before starting the next iteration.**

Figure 21 – DML jobs of applications over distributed workers in networks [b-Xia]

The major content in communication in DML can be viewed as a vector of floating-point numbers describing the model. In contrast to the workflow of type I, the pipeline here needs several iterations to finish training the model with distributed computing over classical networks.

The impact against QC service with respect to network latency and data reliability is thus:

- **Impact of network latency for QC service:** To keep workers' model up to date, the model is synced in every iteration. At the beginning and end of each iteration, multiple flows are generated almost simultaneously to exchange data among workers, generating burst network traffic. Meanwhile, many ML models are trained under strong synchronization requirements, i.e., *all workers need to update their parameters prior to starting next iteration*. Therefore, the performance is determined by the tail completion time of all the flows in one iteration.
- **Impact of data reliability for QC service:** Data loss is likely to reduce the efficiency of convergence during training models. In Figure 21, it is shown that with the increasing of random data loss probability, convergence of the model also needs to be more rounded.

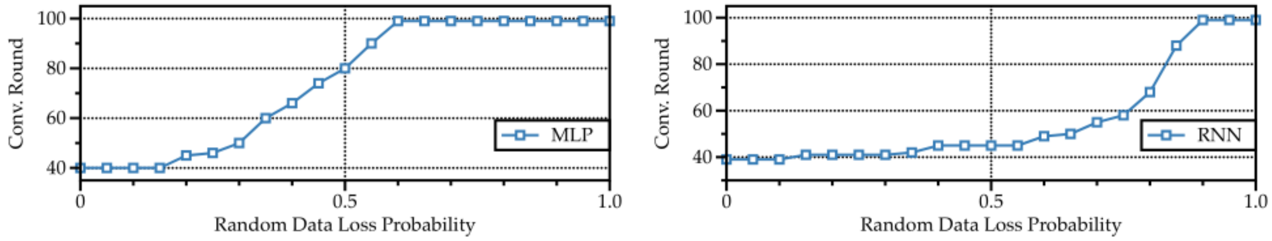


Figure 22 – Impact of data loss on convergence for DML [b-IEEE P3652.1]

Existing ML frameworks rely on existing protocols like TCP or UDP to transmit messages. TCP and its variants seek to minimize the time to transfer all data which inevitably suffers from tail latency even under a tiny fraction of packet delays/losses. UDP, on the other hand, tolerates the tail effect but without the guarantee that at least a certain part of data must be delivered, and this can result in poor eventual accuracy and/or require more iterations to converge.

There are some opening technical solutions for distributed computing as below:

– **Reducing tail latency:** Several research efforts on data centre network areas have been proposed to reduce the tail latency. Pfabric [b-Alizadeh-1] and cutting payload [b-Cheng] optimizes tail latency with fast detection of lost packets. While these methods are effective, they require changes to the switch hardware. TCP based schemes like DCTCP [b-Alizadeh-2] generally improve latency, but they have no guarantee on the worst-case performance.

– **Loss tolerance transport layer protocol:** Some protocols for real-time streaming applications tolerate packet loss, e.g., RTCP [b-Huitema]. However, related applications do not have a strong tolerance bound as ML application does. It remains to be explored whether a dynamic loss tolerance similar to the quality of service (QoS) concept is applicable to DML jobs. Some QC-aware and motivated technical solutions enabled by classical networks are still encouraged to be studied further to improve the quality of QC service.

6.2.5.5 Application prospects

Even at the lowest circuit depth, QAOA offers non-trivial provable performance which is expected to increase with the circuit depth. The QAOA has been proved to be a noise tolerant algorithm. Only with simple quantum circuit structure can QAOA be implemented on NISQ hardware. Therefore, QAOA is a promising quantum algorithm for supporting the quantum supremacy.

The VQE scheme can be applied to solve many kinds of ground state energy problems, and, in the near future, it can be widely used to help chemical synthesis, material designing, drug searching and even road planning, etc. Many calculations that are difficult now may be easily solved with the help of a quantum computer.

6.2.6 Comprehensive analysis and comparison

As shown in Figures 10, 11, 13, 15 and 18, different implementations of computation forms combined with networks are briefly illustrated. Different use cases demonstrate different dependences on quantum technology for computation and communication parts. For example, [UC-QC-004] can be implemented based on classical network overlaid cloud computing infrastructure and software stacks designed for quantum simulators while [UC-QC-002] highly relies on quantum computers and quantum networks such as QIN.

Table 4 – Comprehensive analysis of different use cases

ID	Name	Computation		Networks	Commercial practice	Application maturity
		Server	Client			
UC-QC-001 (Figure 10)	Quantum cloud computing	quantum/ classical	classical	classical	IBM Xanadu, AWS, D-wave, etc.	★★☆
UC-QC-002 (Figure 11)	Distributed quantum computing	quantum	quantum	quantum	None	☆☆☆
UC-QC-003 (Figure 13)	Blind quantum computing	quantum	quantum/ classical	quantum/ classical	None	★☆☆
UC-QC-004 (Figure 15)	Quantum simulator in centralized/ distributed quantum computing	classical	classical	classical	IBM, Google, AWS, Huawei, Alibaba, etc.	★★★
UC-QC-005 (Figure 18)	Hybrid classical and quantum computing	quantum	quantum/ classical	classical	IBM, AWS, Google, D-wave, etc.	★★☆

Based on three aspects of common concerns (see Table 4), the maturity of application is evaluated using criteria on whether the quantum technology is necessary to enable services and applications for QC use cases, considering that quantum computation technology and quantum networking technology are still for further study and not yet standardized. However, there are some quantum-inspired classical technologies such as quantum simulator for computation with high performance provided by IBM, Google, and Huawei etc., which support the demand of potential applications such as microphysics, molecular chemistry and so on. Therefore, if the QC use cases in this technical report can be implemented via classical way in either computation, network or commercial practice, the corresponding maturity of application is marked as one star of ★ for each item.

6.3 Quantum random number generator use cases

Quantum random number generator technology is applicable to many fields. With the advent of quantum mechanics, quantum random numbers which are based on the intrinsic properties of quantum physics are considered to be truly unpredictable random resources that are different from classical random numbers. The following QRNG use cases are described in this technical report:

- **UC-QRNG-001** describes a quantum randomness beacon service for smart contracts.
- **UC-QRNG-002** describes a quantum randomness beacon service for confidential disclosure showing the structure of a beacon service in technical solution.

6.3.1 UC-QRNG-001: Quantum randomness beacon service for smart contract

6.3.1.1 Use case description

Randomness beacon technology utilizes a public randomness service from a trusted third party that meets certain requirements. For the randomness beacon service to be trusted, a beacon must provide full-entropy random numbers that are unpredictable before generation and verifiable after broadcasting.

Contract signing is one use case for the randomness beacon service. For instance, considering a merchandise provider, Alice, who wants to sell some merchandise to Bob at a certain price; if Bob were to accept the quoted price, then Alice and Bob are committed to a contract and perform the transaction. However, it is common that Alice and Bob would not be able to meet in person and would instead prefer to negotiate over the internet. If no special protection is made and they directly communicate with each other, it might be the case where Alice signs the contract and sends it to Bob while Bob delays signing the contract implying that Alice is committed to the contract, but Bob is not.

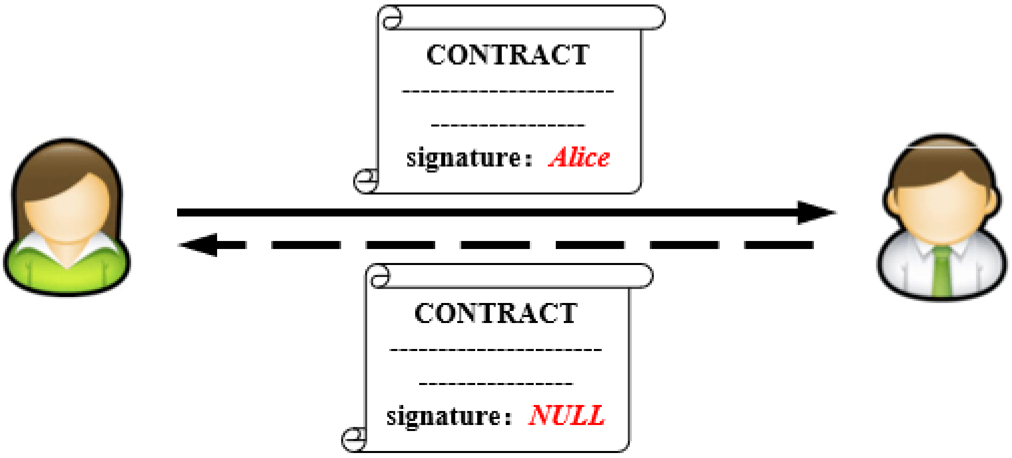


Figure 23 – Alice committed to Bob without Bob's corresponding commitment

To overcome this, a trusted third party, usually an intermediary playing the role of a trusted notary (sometimes performed by the post office), can be involved. Alice and Bob first send their signed contracts to the third party, and it is only when the third party receives both copies that they will send the contracts to Alice and Bob. Alice and Bob are then both committed to the contract. However, this method is highly centralised and since the transaction shall be handed over to the intermediary directly, its liability could be problematic as errors might occur.

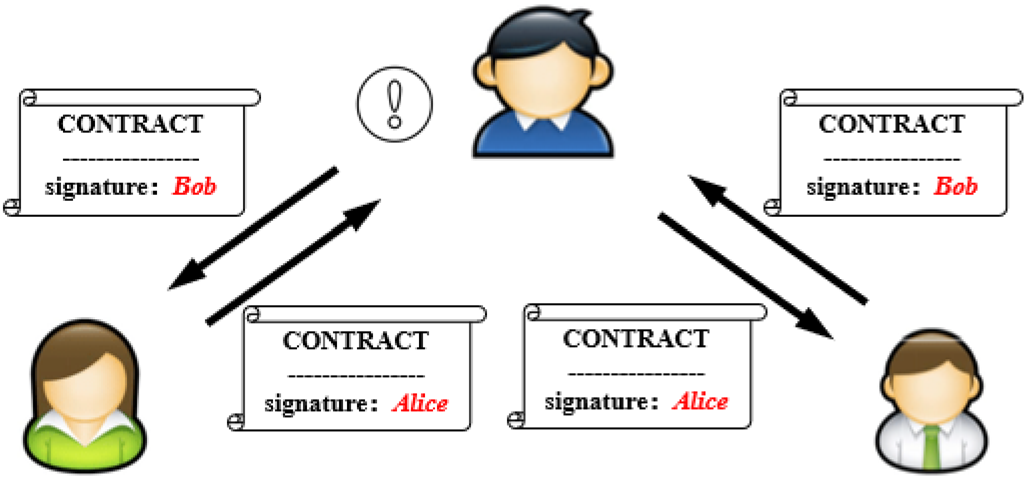


Figure 24 – A centralised solution for contract signing

One solution to the above problem is to employ a trusted third party who provides a randomness beacon service. Alice and Bob shall directly communicate with each other and start the communication at an initial time t_0. They both agree on a random number i and send a singed message of $(i, t_0 + \Delta t)$ to each other (each signs using their own signature that is verifiable by the other party). After this and before the time $t_0 + \Delta t$, they exchange their signed contracts that include i. They repeat the procedure at a regular basis of times proportional to c. For an honest party, he/she stops if the other party does not send the required messages during the respective period, or if the random number they have agreed on during the Δt starting at a time t_f coincides with the random number produced by the randomness beacon at time $t_f + \Delta t$. One party, say Alice, will be viewed as committed to the contract at time$t_f + \Delta t$, only when Bob can:

1) Produce Alice's signed contract

2) Produce Alice's signed message $(i, t_f + \Delta t)$

3) Produce the beacon-signed message $(i, t_f + \Delta t)$

The requirement for Bob to be committed to the contract is the same with the names "Alice" and "Bob" interchanged. Also, the randomness beacon service will always produce a signed random number at time $t_0 + n\Delta t$ $(n = 0,1,2,\cdots)$. If the range of the random numbers is $[0, k-1]$, the expected time for honest parties to be committed to the contract will be $k\Delta t$. On the other hand, if one party, say Bob, intends to cheat Alice, Bob would not send their signed contract to Alice during the period $[t, t + \Delta t]$. The only possible case that Bob would succeed (produces the messages in the requirements presented above which persuades an adjudicating authority that Alice should be committed to the contract) is that the beacon-produced random number at the time $t + \Delta t$ coincides with their agreed random number i at the time t. The probability of this event to occur is $1/k$. This is a smart contract signing protocol allowing to avoid one of the parties to repudiate its commitment with a small failure probability $1/k$ that depends on the range of random numbers produced by the randomness beacon service.

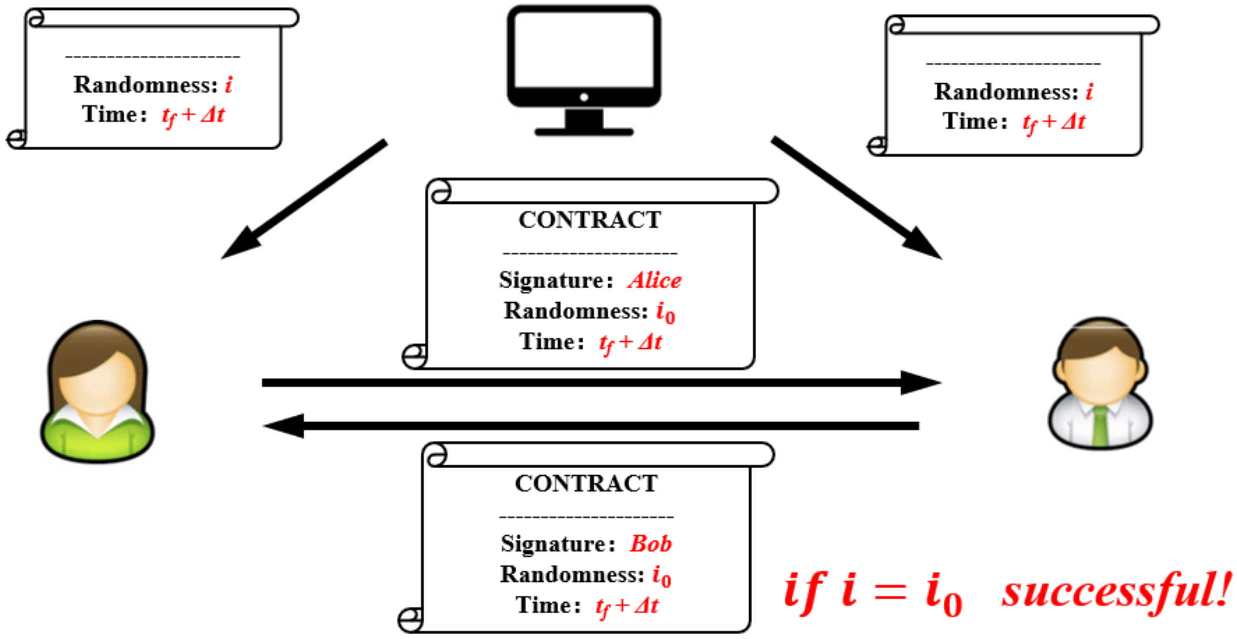


Figure 25 – Randomness beacon utilized for smart contract

With a proper design of a randomness beacon service and potential improvements to smart contracts, the failure probability can be reduced, and efficiency can be improved. Additionally, the service provider of the randomness beacon does not have access to any contract, nor do they receive information on the transactions, they only perform unidirectional broadcasts of signed random numbers to the public. Therefore, they have a limited liability and can support decentralized internet protocols.

Target end users for UC-QRNG-001 include those who have needs for business signatures in e-commerce, anonymous networks (such as blockchain systems) and other services.

6.3.1.2 Problem statement

There are cryptographic secure solutions based on complexity hardness arguments but most of these are not within the reach of current communication technologies. Moreover, their security might be compromised under the threat of a quantum computer. Post quantum cryptographic methods should be evaluated as alternatives that are not hitherto studied.

6.3.1.3 Motivation/advancement

Beacons must provide full entropy random numbers that cannot be predicted before they are generated.

DIQRNG provides ε-true secure private random numbers under the minimal assumptions within current knowledge. The entropy of a DIQRNG source can be rigorously evaluated and state of the art DIQRNG experiments have reached a maturity that is sufficient for a randomness beacon service.

6.3.1.4 Technical solution

Loophole-free DIQRNG can provide verifiable intrinsic randomness without trusting/characterizing the functionality of the (quantum) device. For this reason, DIQRNG is most suitable to meet the requirement of unpredictability of a beacon service. State of the art DIQRNG implementations are close to maturity that is sufficient for a public service. It is for these reasons that this report points out that it is timely to implement DIQRNG as entropy sources for a randomness beacon service.

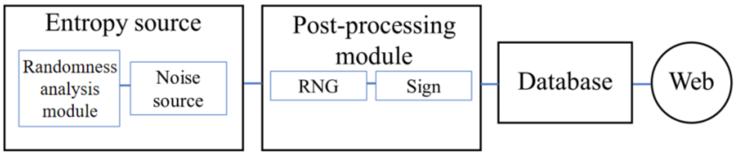


Figure 26 – Structure of a beacon service

6.3.1.5 Application prospects

As a public service, it can be assumed that the potential market size of beacon is similar to that of the existing public key authentication system.

6.3.2 UC-QRNG-002: Quantum randomness beacon service for confidential disclosure

6.3.2.1 Use case description

Consider the situation that Alice, a keeper of a data bank of personal files, agrees to disclose a confidential content DIS to Bob. It is assumed that Alice is responsible for the authenticity of the DIS and Bob agrees to keep it confidential. If DIS denotes the actual string of the secret, referred to by a number *dis*, Alice must be sure that when the secret is disclosed to Bob, Alice will have Bob's receipt for DIS.

Target end users for UC-QRNG-002 include those who need the disclosure of confidential information from data centre.

6.3.2.2 Problem statement

If Alice and Bob communicate with the help of a trusted third party, the situation will result in a dilemma of centralization, since it must be assumed that the third party is trustworthy even when this is not always the case. Thus, the secret DIS may have security risk in the hands of a third party.

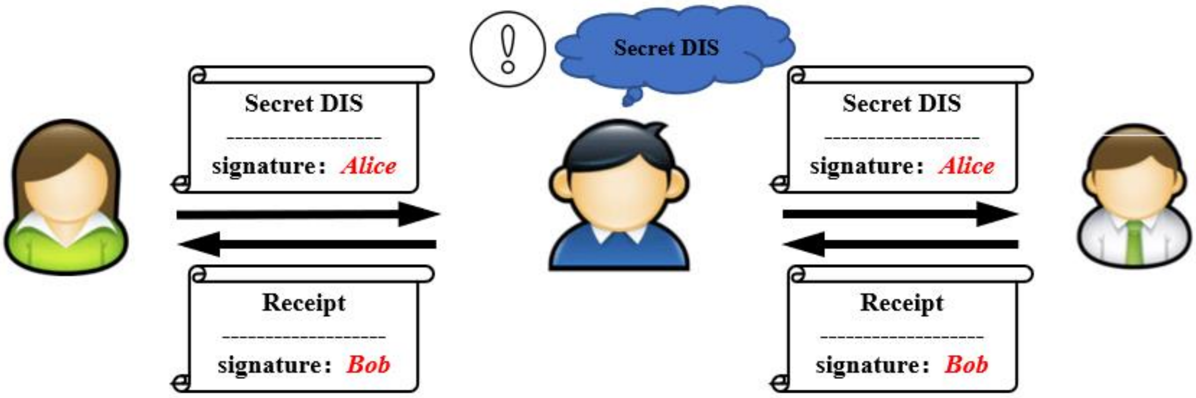


Figure 27 – The security risk in a centralised solution

6.3.2.3 Motivation/advancement

The protocol based on the quantum randomness beacon ensures that the confidential information is kept away from the third party. The provider of the quantum randomness beacon can only broadcast the beacon signal without accessing the confidential information.

6.3.2.4 Technical solution

A disclosure beacon protocol can solve the problem of confidential disclosure without the trusted third party. The randomness beacon service repeats producing a random number i_{BN}, a series of encryption keys $(p_1, \dots, p_k)$ and a decoding key $d = d(p_i)$ with period Δt and broadcasting the signed message of $(p_1, \ldots, p_k, d, t_0 + n\Delta t)$ at time $t_0 + n\Delta t\ (n = 0,1,2,\cdots)$. Alice and Bob start the communication at the initial time t_0. To enforce the protocol, Alice encodes DIS by Bob's encryption key B, followed by their own encryption key A, to produce the result M. They agree on a random number i which Alice takes to choose the i^{th} encryption key in $(p_1, \ldots, p_k)$ released by the beacon at time t_0. Alice encrypts her decoding key $d(A)$ by the key p_i, i.e., $E_{P_i}(d(K))$. After Bob sends the signed receipt $(dis, i, t_0 + \Delta t)$ to Alice (the signature is verifiable by the other party), Alice then sends Bob the signed message of encrypted decoding key $d(A)$ together with dis, i, and t_0. They also repeat the procedure with period Δt.

An honest party stops if the other party does not send the required messages in the respective period, or if the random number i and key p_i they have used during the Δt starting at a time t_f, coincides with the random number i, decoding key $d(p_i)$ released by beacon at the time $t_f + \Delta t$. For the latter case, Bob can decode $E_{P_i}(d(A))$ to get $d(A)$, and then decode M by $d(B)$ and $d(A)$ to obtain DIS.

Bob will be viewed as committed to the receipt at time $t_f + \Delta t$, only when Alice can:

1) Produce Bob's signed reference value dis of DIS

2) Produce Bob's signed message $(i, t_f + \Delta t)$

3) Produce the beacon-signed message $(i, t_f + \Delta t)$

Alice will also pass as provided the secret DIS, unless Bob can:

1) Produce Alice's signed message of encrypted decoding key $E_{P_i}\big(d(A)\big)$

2) Prove that the decoding key $d(A)$ is not for the encryption key A

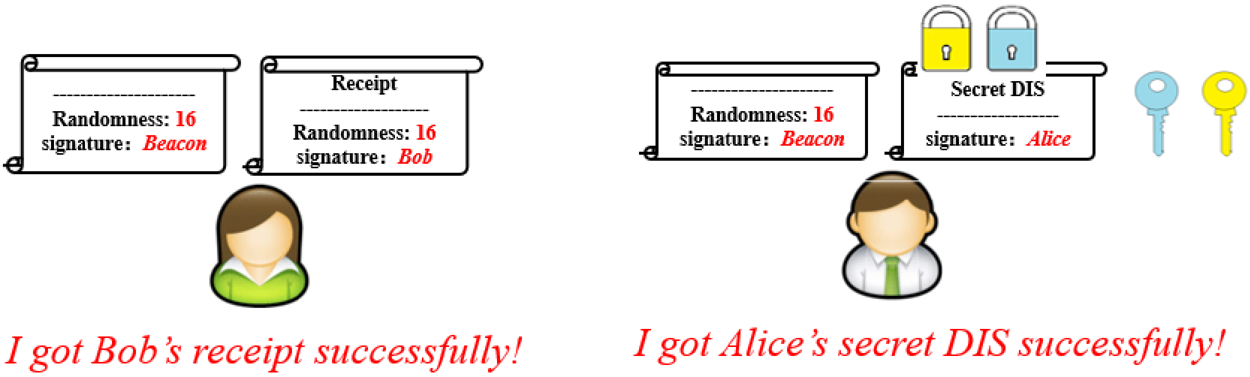


Figure 28 – The judgement of the validity

Also, the randomness beacon service will always produce a signed random number together with encryption keys and decoding key at time $t_0 + n\Delta t\ (n = 0,1,2,\cdots)$. If the range of the random numbers is $[0, k-1]$, the expected time for honest parties to complete the disclosure will be $k\Delta t$. On the other hand, if Alice intends to cheat Bob, Alice will not send the signed encrypted decoding key to Bob during the period $[t, t + \Delta t]$. The only possible case that Alice will succeed is that the beacon-produced random number and decoding key at the time $t + \Delta t$ coincide with their least recently used random number i and key p_i at the time t. Therefore, Alice can produce the messages in the requirements presented above which persuades an adjudicating authority that Bob has been committed to the receipt, escaping from providing DIS for Bob. The probability of this event to occur is $1/k$.

However, if Bob intends to cheat Alice and does not send the signed receipt to Alice, it will immediately lead to the termination of the protocol. Moreover, if Alice can know the beacon message beforehand, Alice can successfully cheat by manipulating their randomness number i to coincide with the beacon-produced random number and not send the signed encrypted decoding key to Bob during the period. It is important to ensure the beacon satisfies unpredictability and authority.

6.3.2.5 Application prospects

In the process of private information transmission, it has great application value; confidential information could be an individual's medical records, tax records, asset information etc.

6.4 Quantum communication use cases beyond QKD

This clause presents quantum communication tasks that will be available at later stages of developments of quantum networks. These stages of developments are characterized by the availability of hardware such as quantum repeaters, quantum memories or entanglement distribution [b-Wehner]. The tasks introduced in this section then become available, with these pieces of hardware added to the quantum network equipment.

The following quantum communication use cases are considered in this technical report:

– **UC-QCOM-001:** Quantum digital signatures

– **UC-QCOM-002:** Quantum anonymous transmission

– **UC-QCOM-003:** Quantum money

6.4.1 UC-QCOM-001: Quantum digital signatures

6.4.1.1 Use case description

Digital signatures allow the exchange of digital messages from a sender to multiple recipients, with a guarantee that the signature comes from a genuine sender. This can be used to authenticate the sender of a message.

The security of quantum digital signatures (QDS) relies on *transferability* (a signature can be transferred to a third party), *non-repudiation* (same as classical) and *unforgeability* (a signature cannot be forged by a third party). QDS are used to sign classical messages but not quantum messages.

Quantum digital signatures can be made unconditionally secure which ensures long-term security and quantum resistance. The security requires the pre-distribution of keys amongst the participants of the protocol. With no prior agreement, the sender could repudiate its messages. In particular, preventing the tampering of a message by the sender after it was signed reduces to the security of bit commitment, a task that cannot be achieved with unconditional security, even using quantum resources [b-Lo].

Classically, digital signatures often rely on public key infrastructures. In the quantum case, more advanced resources are usually involved, such as a trusted key distribution centre. This distribution phase is a strong requirement which mitigates the advantage of unconditional security.

6.4.1.2 Required network stage

The requirements of quantum digital signatures protocol have been decreased by a series of work following the research of [b-Gottesman]. The original protocol assumed non-destructive state comparison and a secure quantum channel; however, these assumptions have now been refuted to assume only a long-time quantum memory [b-Amiri]. Less efficient protocols exist that only require prepare-and-measure operations which are available in QKD networks. These protocols typically require sending very long qubit strings for signing a single bit of information. Nevertheless, they can be implemented with current technology at a small scale or using quantum repeater to reach long distances. End-to-end security and distribution to arbitrary distant parties nevertheless require the use of quantum repeaters.

6.4.1.3 Application prospects

Quantum digital signatures could be used for authenticating network nodes. New threat models appear with the growing number of devices connected to internet, and in particular the increase of

IoT. QDS could be useful for critical IoT devices in industries such as transport, maritime, oil and gas, mining or agriculture, in which updating keys can be difficult. Quantum digital signatures are bringing long-term security to the security of such devices, ensuring that their signatures cannot be counterfeited, regardless of the time these devices remain in use.

Beyond device identification, digital signatures can also be used to guarantee the integrity of stored data. The unforgeability of the signature ensures that the data is stored by a legitimate party and checking the signature guarantees they have not been altered. The quantum benefit is to maintain this guarantee for a long time.

6.4.2 UC-QCOM-002: Quantum anonymous transmission

6.4.2.1 Use case description

Anonymous transmission is a task that enables two nodes to communicate in a network anonymously. More precisely, one of the nodes of the network, the sender, communicates a quantum state to the receiver such that their identities remain completely hidden throughout the protocol. In particular, it implies that the sender's identity remains unknown to all the other nodes whereas for the receiver it implies that no one except the sender knows their identity. The main goal of anonymous transmission is to fully hide the identities of the sender and the receiver but does guarantee the reliability of the transmitted message.

Several classical protocols for anonymous transmission have been proposed since the late 1980s. The most widely spread practical solutions are proxy anonymizers, which are based on trusted third parties, and networks based on computationally secure problems and a chain of forwarding. Famous examples of the latter include MixMaster, PipeNet, OnionRouting and its best-known implementation, Tor.

Quantum protocols for anonymous transmission are traceless, i.e., the sender cannot be reconstructed afterwards; they do not rely on a trusted third party nor use computational assumptions. Moreover, they seem well-suited for small scale infrastructures since they do not require using a chain of servers, unlike the protocols based on chains of forwarding.

6.4.2.2 Required network stage

Various protocols for quantum anonymous transmission have been introduced which differ in the hardware they require. State of the art protocols can be implemented by distributing large, entangled states [b-Lipinska] and [b-Unnikrishnan]. Progress on the generation and distribution of entangled states may allow scaling quantum anonymous transmission to a larger number of parties.

6.4.2.3 Application prospects

Anonymous transmission allows quantum distributed computation to be performed without revealing the identity of the agent that provides the information. It is therefore useful in cases where data from various sources must be aggregated while hiding the identity of the agents providing the data. This is a simplified version of secure-multiparty computing which aims at hiding all information that cannot be deduced from the output of the computation.

For example, monitoring car traffic can lead to a better road management. Drivers, however, might not be willing to share their private information, in particular regarding their speed and position. Quantum anonymous transmission could be used to hide the drivers' identities while collecting valuable data.

Anonymous transmission can be used to design applications that are private by design. This could be interesting to develop GDPR-compliant applications and more generally for the protection of free speech or whistle-blowers. This can be useful for international institutions to enforce human rights by design.

6.4.3 UC-QCOM-003: Quantum money

6.4.3.1 Use case description

The concept of quantum money was first introduced in [b-Wiesner] in 1983. Informally, the quantum money object is a *unique* and *unforgeable* physical object that is created by a third party called *Mint*. Then, it is circulated among potentially untrusted parties called *Holders* who might attempt to forge it for double spending. A merchant, however, upon receiving it, should be able to verify that the money has not been forged and originated from *Mint*. There exist many verification schemes based on different types of communication and types of encryptions used by *Mint*.

Classical decentralized digital currencies are based on the use of a ledger called a blockchain. Operations such as token emission and spending are reported to the public ledger. The ledger is publicly verifiable and copied on several nodes of the network which ensures that no minority of agents can alter the history of operations.

Quantum money does not aim at decentralizing the transaction, but rather to strengthen their security. Quantum resources lead to tokens whose integrity can be verified by anyone, but that can only be spent once. Like for QKD or QDS, the security of these tokens is unconditional. Moreover, since there is no need for a ledger, the quantum solution has a better scaling. While classical digital currencies can be fully decentralized, quantum money is emitted by a *Mint* which is a central authority.

6.4.3.2 Required network stage

In most cases, quantum tokens need to be stored. This implies the use of quantum memories that can hold quantum information for a long time. There exist several proposals to implement quantum money with various hardware requirements and security properties [b-Gavinsky], and reaching different trade-offs between security, efficiency and required technology.

6.4.3.3 Application prospects

Quantum money has interesting properties for identifying IoT devices. One solution to manage the identity of such devices is to hardcode a master key in them. Such devices are assumed to be light, and their identity credentials could be stolen or copied. The various proposals for quantum money protocols are all based on the idea of producing unforgeable tokens. The security of these construction is derived from the unclonability of quantum states, a physical property that ensures the security of many quantum tasks. Moreover, quantum tokens are, like standard money, issued by a central authority but can also be revoked easily. One difference, however, is that when quantum tokens are consumed, they are not available anymore while authentication may be needed several times.

The unforgeability and unclonability of quantum money could be helpful to design secure operations running across different blockchains. More precisely, the main security risk when transferring tokens from one blockchain to another is that the tokens could get copied during the operation, allowing double-spending. Quantum coins can only be spent once which seems to offer a solution to this problem.

7 Key findings and suggestions

7.1 Quantum time synchronization

7.1.1 Technical advantages of QTS

Based on the analysis in *Clause 6.1*, higher accuracy of time synchronization better than tens of ns, even ps level will be required in the future, e.g., 5G advanced and 6G applications, metre and sub metre level positioning services of IoT. In addition, the security issue has drawn more attention due to various attacks on the time synchronization protocols. The application of quantum technology in time synchronization can achieve precision or function that cannot be achieved by classical methods such as:

- **Higher accuracy:** With emerging advanced quantum technology-based clock source (e.g., optical clock) or/and quantum entanglement transmission technology it is expected to improve the accuracy of time synchronization by thousands of times, in the principle experiment of UC-QTS-001, the precision of time synchronization can reach picosecond or sub-picosecond level.
- **Security enhancement:** Classical encryption technology is difficult to resist delay attacks against time synchronization protocol while quantum technology, e.g., UC-QTS-002 can resist protocol packet attacks and delay attacks at the same time.

7.1.2 Key enabling technology

The key technologies involved in quantum synchronization mainly include:

- **Atom/ion manipulation** (used in UC-QTS-001 – optical clocks): including atom/ion capture and cooling, state selection, Ramsey interference and detection, etc.
- **Preparation and distribution of entanglement source** (used in UC-QTS-001 – quantum synchronization protocol, UC-QTS-002 and UC-QTS-003): quantum entanglement source is the key enabling device to realize quantum synchronization protocols and a quantum clock network. High quality deterministic quantum entanglement preparation and distribution as well as high-dimensional quantum entanglement manipulation will be the first controlling factor to realize quantum synchronization technology. Appendix II provides some additional material on the quantum light source for further information.
- **High order quantum correlation detection** (used in UC-QTS-001 – quantum synchronization protocol): including coincidence measurement, second-order interference (HOM), etc.
- **Quantum synchronization protocols:** taking advantage of quantum entanglement and high-order correlation characteristics to break through the classic shot noise limit thereby improving synchronization accuracy. So far, three main types of QTS protocols have drawn much attention but are still under research:
  1. *Round trip protocol:* There is no need to measure the arrival time of the signal to avoid the measurement error and the dispersion effect of the fibre is eliminated due to round trip of optical path.
  2. *One way protocol:* The accuracy depends on the measurement accuracy of the arrival time of the signal. It is suitable for long distance time synchronization applications.
  3. *Two-way protocol:* There is no need to measure the arrival time of the signal and it can resist the influence of dispersion effect.

7.1.3 Maturity and application prospects

Quantum synchronization technology is still in the laboratory stage. Its future commercial deployment mode requires further exploration.

Some key technologies of quantum synchronization need to be broken through. For example:

- In the quantum synchronization clock network (UC-QTS-003), it is necessary to establish or distribute multi entanglement resources in advance or establish multi entanglement in a similar way to quantum teleportation. At present, the preparation and long-distance distribution of high-quality entanglement sources are still in the stage of laboratory exploration.

- Some quantum synchronization protocols (UC-QTS-001) require a series of quantum gate operations on qubits. This puts forward higher requirements for the accuracy of quantum gate operation and quantum decoherence time. With further research and development of quantum computing, the application and deployment of this part of the technology may be promoted.
- Emerging optical clock needs further improvements in aspects such as optical clock service time, optical clock comparison, distribution of optical clock source reference, etc. before it becomes a practical and widely adopted clock source/timescale.

At present, quantum synchronization technology cannot be deployed and worked independently from classical network resources. For example:

- Quantum synchronization technology needs to use classical network to transmit necessary information. In quantum synchronization clock network (UC-QTS-003), the synthesized frequency and error signal need to be transmitted through a classical channel while for the quantum synchronization protocol (UC-QTS-001), the classical channel is used to transmit information such as the pulse arrival time.
- The remote comparison of quantum clock sources (such as optical clock in UC-QTS-001) also need the help of classical channels, such as wireless satellite or optical fibre channels.
- Qubits (UC-QTS-001 and UC-QTS-002) can also be transmitted in the same optical fibre as the classical signal in the form of wavelength division multiplexing, similar to QKD technology.

When quantum synchronization technology is applied in a classical network, it puts forward some new requirements for the classical network. For example:

- In the roundtrip time synchronization protocol (UC-QTS-001), the time-varying delay needs to be inserted and the precision of the variable delay directly determines the synchronization precision. Therefore, the necessary electromechanical control technology needs to be introduced into the classical network.
- Some quantum synchronization protocols (UC-QTS-001) based on HOM interferometer need to balance the two transmission paths and they also require variable delay or variable refractive index in the link and real-time feedback adjustment.
- The accuracy of one-way time synchronization protocol (UC-QTS-001) is sensitive to the delay jitter of the transmission link. It is well known that optical fibre deformation caused by temperature, stress and other factors will lead to the change of transmission delay jitter. Thus, if one-way synchronization protocol is applied, the delay jitter of transmission link needs to be improved.
- When the optical clock (UC-QTS-001) is introduced into the classical network, since the optical frequency is very high, the traditional electronic frequency counter cannot detect this frequency signal. Therefore, the optical band signal must be converted to the microwave band implying some new functional components such as optical frequency comb, need to be introduced.
- Frequency synchronization network needs high-precision frequency monitoring technology to realize the management system, including alarm generation or switching trigger caused by frequency signal degradation. Traditional synchronization networks need a higher quality clock source to monitor the quality of frequency signals. However, the optical frequency signal generated by high-precision optical clock (UC-QTS-001) is too accurate to be evaluated by the absolute value of other clocks. To determine the error of high-precision optical frequency signals, a majority decision and relative monitoring based architecture such as coherent network PRTC (cnPRTC) will be effective and could be considered. The optical clock remotely compares itself to the optical clocks of other sites through the network/optical fibre link to monitor whether the frequency signal is degraded so as to trigger alarm or switching, as discussed in clause 6.1.1.

Quantum synchronization technology can provide high-precision synchronization services for classical networks.

- Optical clocks (UC-QTS-001) can provide high-precision frequency synchronization service for classical communication networks. For example, frame slip may occur between devices connected to different clock sources in the transmission network (such as SDH network) because the frequency difference between clock sources is too large. For example, if the frequency difference between clock sources is in the order of 10e-6, it can be estimated that the frame slip occurs once in about 62.5 s (125 us / (2×10e-6), where 125 us is the SDH frame period). Therefore, the traditional frequency synchronization network adopts the master-slave network architecture and the network equipment are synchronized with a few primary reference clocks (PRCs) to avoid the frame slip effect caused by the difference between clock sources. The precision of the optical clock is very high which can reach the order of 10e-18. If the optical clock is used as the clock source, the interval of frame slip will be estimated as two million years, so there is no need to consider the problem of frame slip in the whole lifetime of the equipment.
- When nodes in classical networks need to achieve ultra-high precision time synchronization, such as sub ns or ps synchronization, quantum synchronization technology (UC-QTS-001) can provide such a service which cannot be achieved by classical synchronization technology.

Generally speaking, there are many technical routes of quantum synchronization technology. Many key enabling technologies are still in the laboratory stage, but their technical advantages are showing huge application potential. Moreover, future applications and deployments still need further in-depth research and exploration. Therefore, cooperation with other R&D entities or standards bodies (inside or outside ITU-T) is highly encouraged to explore more potential applications of higher accuracy for time synchronization in real networks and to facilitate the development of key enabling technologies.

7.2 Quantum computing

7.2.1 Technical advantages of QC

Based on the comprehensive analysis of clause 6.2, compared to classical computing, quantum computing shows such potential technical advantages as:

- **Exponential acceleration for computation:** As mentioned in UC-QC-001, quantum computing is usually described in a quantum circuit model with N qubits which can be spanned into a $2^N \times 2^N$ matrix space mathematically. All the computation states can be naturally operated and refreshed in parallel taking advantage of quantum physical properties. Moreover, according to UC-QC-002, the tensor-product-like coupling of the joint quantum computing network generates computational advantages over the simple sum of separated individual chips' capability.
- **Improving computational efficiency:** In UC-QC-002 and UC-QC-005, it is shown that some promising quantum algorithms such as VQE, QAOA, QA and so on could be running on NISQ hardware, in which specific combinatorial optimization problems, linear equations and factoring problem are formulated to find the ground states of some special Hamiltonian. Quantum computing explores an energy-based method to find optimal solution more efficiently comparing to classical computing under quantum physical system.

7.2.2 Key enabling technology

The key enabling technologies of quantum computing are summarized as:

- **Quantum computing chip or device:** As the core part of a quantum computer, the quantum chip or device is essential to perform quantum computing and quantum information processing with quantum computing software.

- **Quantum algorithm:** To develop the significant advantage of a quantum computer for application, smart and effective algorithms should be designed to be suitable for specific quantum computing architecture.
- **Quantum simulator:** According to UC-QC-004, an equivalent quantum circuit model can be derived and simulated on a classical computer or a cluster of classical computers. Quantum simulators are **crucial** before quantum devices are mature enough and robust to noise. In addition, emerging quantum (circuit) simulators over classical networks will support creative, cutting-edge research in science and engineering to uncover new paradigms, advance nascent hardware platforms and develop new algorithms, software and applications for a new generation of quantum simulators.
- **Classical networking enhancement for quantum computing:** According to UC-QC-004 and UC-QC-005, after receiving the computing tasks, the servers can run the classical portion in local resources or schedule other remote computing resources (CPU/GPUs) over a typical network (e.g., TCP/IP) to execute these tasks. **However**, existing networks are not carefully designed for quantum computing applications such that there are some new technical requirements for classical communication networks such as big data traffic and communication overhead, deterministic delay and/or low-latency, high security and privacy, reliability or robustness, etc.
- **Quantum networking interconnection of quantum computers:** According to UC-QC-002, the computational power of a single quantum chip is limited by the number of qubits and the topological complexity of the chip. It is predicted that connecting different quantum chips into a network may **yield** a computational power greater than the simple sum of the computational power that individual chips have. Moreover, in UC-QC-003, several protocols are proposed for further study to execute quantum computation between quantum servers and quantum/classical clients.

7.2.3 Maturity and application prospects

Presently, quantum advantage/supremacy has been achieved in experimental demonstration. In the next few years, NISQ devices with around a hundred qubits will be available to begin experiments with the possibilities provided by quantum computers. However, the full potential of quantum computers may need to experience a long period of development. There are several different possible technological candidates for qubit implementations and networking connections, however, it is quite unclear what the most mature technical solution is. In general, the development of both quantum computing and quantum networking are still at very early stages.

Potential applications based on NISQ computational framework are actively explored in both academia and industrial area, e.g., VAE based quantum chemistry/ molecular simulations, QAOA or QA optimization problems etc. After the discussion of QC use cases, it is found that QCC may likely provide a commercial service via traditional or quantum internet where some applications can be implemented by a simulator and/or real quantum computing hardware in the future. In general, there are two promising ways to transfer the quantum portion of applications or programs to quantum computers:

1) The classical computer generates the compiled quantum assembly program locally and sends it to the quantum computer over the classical network. The quantum computer generates the required quantum data specified by the assembly program and performs the related quantum computation. The result is returned through the classical network.
2) The classical computer also sends the quantum assembly program via the classical network but generates the required quantum data in quantum random access memory (QRAM) and sends them to the quantum computer via the quantum network. The quantum computer runs the quantum assembler program directly based on the data received from the quantum network. The result is also returned through the quantum network.

According to the analysis and basic conclusion of clause 6.2.6, quantum simulator for centralized/distributed quantum computing (UC-QC-004) is relatively mature in computation, network and commercial practice. It is suggested to further study corresponding scenarios, key components, networking techniques, standardization requirements in related areas of advanced computation and future network jointly between ITU-T Study Groups, e.g., ITU-T SG13 and other SDOs.

7.3 Quantum random number generator

7.3.1 Technical advantages of QRNG

With the development of quantum mechanics, quantum random numbers based on the intrinsic properties of quantum physics are considered to be a truly unpredictable random resource different from classical random numbers. Quantum random numbers are a relatively mature technology, and the architecture of quantum noise random number generator has been recommended in [b-ITU-T X.1702].

Typical QRNGs, i.e., device-dependent QRNGs require a detailed characterization of their operation to ensure the quality of their output. While DIQRNG can provide true randomness without the assumption of the inner working of the device, ensuring the conditions are met places a significant burden on the user. So far, various QRNG schemes have been proposed and demonstrated and there are a variety of commercial products which have been on sale. According to the required reliability of the device, QRNG can be divided into three categories: DIQRNG, semi-DIQRNG, and device-dependent QRNG. Their practicality and security are illustrated in Figure 21.

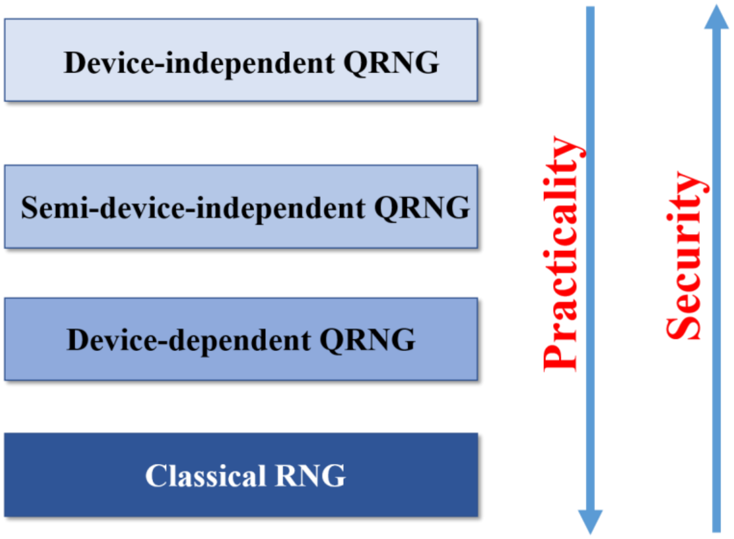


Figure 29 – Practicality and security of different RNG categories

DIQRNG can produce certified randomness without trusting devices. Hence, DIQRNG is regarded as the most secure QRNG and its characteristics include:

– **Self-testing:** Randomness is certified independent of device implementations and against general adversaries.

– **Unpredictable:** The output numbers cannot be predicted according to the antecedent sequence numbers or given access to any other information about the system.

– **Uniformity:** The output numbers are uniformly distributed.

7.3.2 Key enabling technology

The key enabling technologies of QRNG are summarized as:

- **Quantum source:** The quantum entropy source which is used to prepare the quantum entropy.
- **Quantum state measurement:** Applying a measurement to the entanglement state with randomly selected measurement settings.
- **Entropy verification:** The non-local test, defined by the distribution of the input and output of the system, can be used to verify if the system performs stable.
- **Extraction of randomness:** An extractor is used to generate strong randomness from the raw data.

7.3.3 Technology maturity of DIQRNG and potential future directions

- **System development:** A prototype of DIQRNG has been built in the laboratory which can generate a safe random number without assumptions about the inner working of the devices.
- **Performance:** The production rate of device-independent random numbers can be achieved is around 2000bits/s so far, and there is a lot of room for improvement in the future.
- **Technology promotion:** At present, the technical threshold of DIQRNG is slightly high which makes the cost of large-scale promotion high. However, at the technical level, DIQRNG is ready for the public service.
- **Future directions:** Providing the beacon service in combination with the internet as a public service is conducive to information security.

With the rapid development of quantum information technology, the research of the generation, practicality and standardization of DIQRNG will be very helpful to provide a truly reliable source of randomness for QKD and other fields requiring high-security random input. The establishment of a unified standardization will play an important guiding role in promoting commercialization and industrialization and is the key to the subsequent development of this field.

7.4 Quantum communications

7.4.1 Technical advantages of QCOM

Based on the analysis of use cases presented in *Clause 6.4*, the following security properties were identified:

- **Everlasting security**: the impossibility for an adversary to break a quantum communication protocol in the future, after its execution.
- **Unforgeability**: the impossibility to create illegitimate quantum tokens.
- **Traceless transmission**: the impossibility to reconstruct quantum communication paths.

These security features are much stronger for quantum protocols than for their classical counterparts. In most cases, quantum protocols allow unconditional security, i.e., security that does not rely on the computational hardness of a mathematical problem. In consequence, quantum communication can reach very high security guarantees for practical problems.

7.4.2 Enabling technologies

The use cases presented in *Clause 6.4* make use of various hardware for quantum technologies. For practical purposes, the following pieces of hardware will be required:

- **Quantum repeaters**: A device that can increase the distance of quantum communication. This will be needed to achieve end-to-end distribution of quantum states.
- **Quantum memories**: A device that can store quantum information of an arbitrary amount of time and convert its quantum state into a flying qubit suited for communication.

- **Quantum entanglement distribution devices**: A device that can generate and distribute arbitrary quantum states on-demand.

7.4.3 Maturity and application prospects

The hardware required for the implementation of the quantum communication use cases is still at a very low technology readiness level. While some implementations of these use cases have been done in lab environments, these used simplified setups to bypass the need for unavailable hardware.

On the other hand, all these hardware are required for future quantum computers. The stages of development of quantum communication networks required to deploy those use cases thus stand in between the current stage (QKD networks) and a large-scale quantum internet that would connect quantum computers with quantum communication channels.

Appendix I

Overview of use cases

This Appendix provides an overview of the QKDN use cases considered by the Focus Group on Quantum Information Technology for Networks.

I.1 Quantum time synchronization use cases

I.1.1 Quantum time synchronization in telecommunications

Use case ID	UC-QTS-001
Contributors	Bin Luo, Chengbin Wu, JiDong Xu and Yuan Gu; *ZTE Corporation* Meng Zhang; *China Academy of Information and Communication Technology (CAICT)* Chung Xu Zhao; *China Unicom*
Short description	This use case provides high precision time reference from clock source/time server through communication network nodes to end devices/systems for specific applications (e.g., base station).
Target end users	Communications operator, time centre.

I.1.2 Secure quantum clock synchronization

Use case ID	UC-QTS-002
Contributors	Meng Zhang; *China Academy of Information and Communication Technology (CAICT)*
Description	Secure quantum clock synchronization is introduced to realize safe and reliable transmission of synchronization information to the end node. This use case is applicable to communication network, industrial Internet and other time-sensitive network applications.
Target end users	Communications operator, time centre.

I.1.3 A quantum network of entangled clocks

Use case ID	UC-QTS-003
Contributors	Meng Zhang; *China Academy of Information and Communication Technology (CAICT)*
Description	A quantum clock network that uses non-local entangled states can realize shared high precision (near the fundamental precision limit by quantum theory) timing by combining precision metrology and quantum networks for some applications like satellite navigation.
Target end users	National time service center, Telecom operators, etc.

I.2 Quantum computing use cases

I.2.1 Quantum cloud computing

Use case ID	UC-QC-001
Contributors	Bo Lv; *China Academy of Information and Communication Technology (CAICT)* Man-Hong Yung and Xiao-Dong QI; *Huawei Technologies Co. Ltd., China*
Description	Potential applications range from basic research to commercial use such as big-data processing, artificial intelligence (AI), material design, and traffic flow optimization. One well-known application of quantum cloud computing is variation quantum Eigen (VQE) solver-based quantum chemistry simulations, where a classical computing server (cloud) is iteratively used to adjust control parameters of a quantum chip to find the energy spectrum of a given chemical structure. The result of the VQE simulation can be used for medicine design, oil processing and so on
Target end users	Researchers, students, governmental organizations, and private companies interested in the study and use of quantum computing techniques for research, education, and industry applications.

I.2.2 Distributed quantum computing

Use case ID	UC-QC-002
Contributors	Bo Lv; *China Academy of Information and Communication Technology (CAICT)* Man-Hong Yung and Xiao-Dong QI; *Huawei Technologies Co. Ltd., China*
Description	This use case employs quantum computing technologies based on a distributed network of quantum devices to run quantum algorithms. Its applications cover both basic research and commercial uses like big-data processing, artificial intelligence, material design, and optimization of complex systems, etc.
Target end users	Quantum device owners, researchers, students, governmental organizations and companies interested in the study and use of quantum computing techniques for research, education, and commercial applications.

I.2.3 Blind quantum computing

Use case ID	UC-QC-003
Contributor	Man-Hong Yung; *Huawei Technologies Co. Ltd., China*
Description	Focusing on enhancement of security and authorization schemes for computation and data when running quantum computing over networks, its applications cover both basic research and commercial uses like big-data processing, artificial intelligence, material design, and optimization of complex systems, etc.
Target end users	Quantum device owners, researchers, students, governmental organizations and companies interested in the study and use of quantum computing techniques for research, education, and commercial applications.

1.2.4 Quantum simulator in centralized/distributed quantum computing

Use case ID	UC-QC-004
Contributor	Bo Lv; *China Academy of Information and Communication Technology (CAICT)* Man-Hong Yung; *Huawei Technologies Co. Ltd., China*
Description	Recent technical advances have brought us closer to realizing practical quantum (circuit) simulators: engineered quantum many-particle systems that can controllably simulate complex quantum phenomena. Quantum simulators can address questions across many domains of physics and scales of nature, from the behaviour of solid-state materials and devices, chemical and biochemical reaction dynamics, to the extreme conditions of particle physics and cosmology that cannot otherwise be readily probed in terrestrial laboratories.
Target end users	Quantum device owners, researchers, students, governmental organizations and companies interested in the study and use of quantum computing techniques for research, education, and commercial applications.

1.2.5 Hybrid classical and quantum computing

Use case ID	UC-QC-005
Contributors	Bo Lv and Zi Shan Liu; *China Academy of Information and Communication Technology (CAICT)* Man-Hong Yung and Xu Shen Xu; *Huawei Technologies Co. Ltd., China* Shuai HAN, Mao-Sheng LI, Jia-Qi HU and Xiao-Wei LI; *Southern University of Science and Technology (SUSTech), China*
Description	QAOA is a variational based quantum-classical hybrid algorithm to solve combinatorial optimization problems in near-term gate-based noisy intermediate-scale quantum computer. The original form of QAOA aims at finding the ground states of some special Hamiltonian, which encode the solutions of specifying combinatorial optimization problems such as Max-Cut problem, satisfiability problems (SAT). More recently, QAOA is developed as the quantum alternating operator ansatz which can also be useful for tackling those problems with some constraints such as the max independent set, traveling salesperson problem. In addition, QAOA is also found to be helpful for solving the problems of linear equations and factoring problem.
Target end users	Quantum device owners, researchers, students, governmental organizations and companies interested in the study and use of quantum computing techniques for research, education, and commercial applications.

I.3 Quantum random number generator use cases

I.3.1 Quantum randomness beacon service for smart contract

Use case ID	UC-QRNG-001
Contributors	*Jinan Institute of Quantum Technology*
Description	This technology – randomness beacon –utilizes public randomness service from a trusted third party that meets certain requirements, or the randomness beacon. In order that the randomness beacon service is trusted, a beacon must provide full-entropy random numbers that are unpredictable before generation and verifiable after broadcasting.
Target end users	Users who have needs for business signatures in e-commerce, anonymous networks (such as block chain systems) and other services.

I.3.2 Quantum randomness beacon service for confidential disclosure

Use case ID	UC-QRNG-002
Contributors	*Jinan Institute of Quantum Technology*
Description	Consider the situation that Alice, a keeper of a data bank of personal files, agrees to disclose a confidential content DIS to Bob. It is assumed that Alice is responsible for the authenticity of the DIS, and Bob agrees to keep it confidential. Let DIS denotes the actual string of the secret, referred to as a number dis. Alice must be sure that when she discloses the secret to Bob, she will have his receipt for DIS.
Target end users	Those who need the disclosure of confidential information from data centre.

I.4 Quantum communications use cases

I.4.1 Quantum digital signatures

Use case ID	UC-QCOM-001
Contributors	*VeriQloud*
Description	Digital signatures allow the exchange of digital messages from sender to multiple recipients, with a guarantee that the signature comes from a genuine sender. Quantum digital signatures can be made unconditionally secure, which ensures long-term security and quantum resistance.
Target end users	For critical IoT devices in industries such as transport, maritime, oil and gas, mining or agriculture, in which updating keys can be difficult.

I.4.2 Quantum anonymous transmission

Use case ID	UC-QCOM-002
Contributors	*VeriQloud*
Description	Anonymous transmission is a task that enables two nodes to communicate in a network anonymously. More precisely, one of the nodes of the network, the sender, communicates a quantum state to the receiver such that their identities remain completely hidden throughout the protocol. It implies that the sender's identity remains unknown to all the other nodes, whereas for the receiver it implies that no one except the sender knows her identity.
Target end users	Useful in cases where data from various sources must be aggregated while hiding the identity of the agents providing the data.

I.4.3 Quantum money

Use case ID	UC-QCOM-003
Contributors	*VeriQloud*
Description	Classical decentralized digital currencies are based on the use of a ledger called a blockchain. Operations such as token emission and spending are reported to the public ledger. Quantum money does not aim at decentralizing the transaction, but rather to strengthen their security. Quantum resources lead to tokens whose integrity can be verified by anyone, but that can only be spent once.
Target end users	Could be helpful in designing secure operations running across different blockchains.

Appendix II

Quantum light source

A QIN transmits information using electromagnetic waves in quantum states, i.e., quantum light. Similar with the classical fibre and wireless network, the performance of the light source is critical to achieve fully functional, high speed and high-fidelity QIN protocols. Based on the technical requirements of different types of QINs such as communication speed, photonic channel type, multiplexing, relay and interface techniques, etc., different specifications of the quantum light source (QLS) are needed. Moreover, the availability of high quality QLS techniques also determine the functionality, implementation and further development of QINs. As a result, the implications of QLS need to be considered during the standardization of all related QIN techniques.

An example of a QKDN based on photonic repeaters is given below to illustrate the implications of a QLS on this particular network.

According to the protocol proposed in [b-Azuma], a special entangled state (cluster state) can be used in each source repeater node to efficiently relay the quantum states from one site to another over long distances. The performance of this repeater network, i.e., the distances between adjacent nodes, communication rate and fidelity, is determined by the aforementioned properties of the QLS. Two numerical examples are given according to [b-Azuma]:

1) For a QKD network with a distance of 4 km between adjacent source repeaters (1000 km overall distance), to achieve a 58 kHz communication rate, an entanglement scale of 38 arms (a graph structure of the cluster) needs to be generated in a rate of 344 kHz in each node, consuming 4.1×106 single photons to establish an entangled pair between the two end nodes. With an estimated quantum error rate of 2.8×10^{-5}, which is jointly determined by the source fidelity, encoding methods, frequency and the transfer medium, the communication fidelity can achieve 0.97◦ .

2) If the distance between adjacent source repeaters is increased to 8 km (with same overall distance of 1000 km) with a doubled quantum error rate, to achieve similar communication rate and fidelity, a 42-arm cluster state needs to be generated for 327 kHz, consuming 7.3×106 single photons for each entangled pair between the two end nodes.

Current QLS techniques include:

- **Using weak coherent state laser as QLS**: Light emitted from a laser is a coherent state light, in which the number of photons contained follows the Poisson distribution. The probability to find n photons in the state is $P_n = (\mu^n e^{-\mu})/n!$, in which μ denotes the average photon number. In its application in a QKD network, μ needs to be reduced to close to 0, such that the probability that the light contains more than 1 photon at a given time is close to 0. However, some special communication protocols, such as decoy state scheme, are necessary to compensate for the non-zero probability of multiphoton photons that may introduce loopholes in the security of the communication.
- **Using two-level system as QLS:** A single system with two energy levels can spontaneously emit a single photon only after being excited with a pump laser. The quantum state of light can be deterministically generated and is a pure single photon state in theory. System such as single atoms, ions, molecules, quantum dots and nitrogen-vacancies in a diamond can all serve as such two-level systems. Among those systems, the self-assembled semiconductor quantum dot predominates as it can produce single photon states that are close to transform limit thereby indistinguishable. Moreover, it provides an interface between a flying qubit (photon) and a solid-state qubit (spin state of an electron or a hole). It has been shown that cluster states (an entanglement state that is robust to errors) can be efficiently generated using single semiconductor quantum dots.

- **Using parametric process as QLS**: Two types of parametric processes are widely used to produce entangled photon states, namely spontaneous parametric down conversion (SPDC) and spontaneous four-wave mixing (SFWM). The former one converts a photon with higher frequency into two photons with lower frequency (therefore lower energy) that are entangled in time, polarization and frequency. The later one converts two independent photons into two new photons that are similarly entangled. During both parametric processes, the energy and momentum are conserved. Both processes involve the usage of nonlinear medium. The main problem of using such mechanism is the non-zero probability to generate photon states with higher photon number, therefore introducing errors to target quantum states. Another application of parametric process as QLS is to convert the frequency of a single photon generated by various platforms to values that are compatible with others.
- **Using squeezed state as QLS**: For a coherent state that a laser generates as mentioned above, an amplitude quadrature and a phase quadrature can be defined, which form a so-called canonically conjugate pair that follows the Heisenberg uncertainty principle. Such states are commonly called continuous-variable quantum states because, instead of having discrete states as other QLS discussed above, the squeezed states have continuous values and therefor forms an infinite-dimensional state space. The main advantage of using squeezed state is that it can be generated using optical parametric oscillators and be measured with homo-dyne detection, during which no low temperature and single photon detection are needed. Entanglement operations such as teleportation and cluster state generation has been demonstrated. Recently, it has been shown that distributed sensing in a quantum network can be realized using squeezed states. Due to the continuous nature of such states, they are more sensitive to noises compared with other QLS techniques.

The implications of QLS on QINs, according to the various properties of QLS, are listed below:

- **Fidelity:** The overlap between the quantum state emitted by a QLS and the desired quantum state is quantified by the fidelity. The communication error of a QIN is proportional to the deviation of the QLS's fidelity [b-Meraner]. In some cases where single photon sources are necessary, two specific characteristics related to fidelity, namely purity and indistinguishability, are especially important to the security and error of a QIN. The purity characterizes the number of photons emitted by the QLS in a given time. In a quantum key distribution network, beam-number splitting attacks may be used by the eavesdropper if the purity of the QLS is not ideal. The indistinguishability describes the extent of how similar two arbitrary photons generated by the QLS are in their wave function, which guarantees the interference visibility of these photons with each other or with other quantum systems. For instance, during the operation of entangling two quantum memories in a QIN, the indistinguishability of photon determines the success probability of entanglement, therefore the ability of remote communication [b-Meraner].
- **Encoding method:** Various methods exist to encode the quantum information into the quantum state of light, such as polarization, phase, time-bin, angular momentum and squeezed state. The fidelity of quantum state of light during the transmission are closely related to the encoding method, which should be determined according to the robustness of the quantum state of light against noises in the transfer medium. For instance, compared with the polarization encoding scheme, it is reported that the time-bin protocol shows better robustness to the turbulence caused by the birefringence in optical fibre channel birefringence [b-Xavier]. Furthermore, high-dimensional encoding method may also increase the information capacity carried by each photon, thus increasing the communication efficiency of a QIN [b-Mirhosseini].

- **Brightness (photon rate):** The highest photon rate that a QLS can generated directly determine the communication speed of a QIN. For particular QLSs and encoding schemes, the photon rate may be intrinsically constrained. For instance, the maximal photon emission rate of a QLS based on a two-level system is determined by the relaxation time of the system from the excited state to the ground state. Meanwhile, sometimes compromises needs to be made between the photon rate and the fidelity of each photon using some particular QLS techniques.
- **Entanglement:** In some QINs which involve the distribution of entangled photons, size, structure and persistency of the entanglement states will greatly impact the performance of the QIN. For example, in a photonic quantum repeater, a special QLS for entanglement state, i.e., cluster state photon source, are required. The number of photons that can be entangled in such a state determines the overall communication distance that photonic quantum repeaters can extend [b-Azuma].
- **Frequency:** In distributed quantum computing or quantum memory network, the quantum light helps to establish entanglements between different nodes that may be remotely located. In most cases, the quantum systems are not able to produces quantum state of light that is suitable for low-loss transmission in fibre. For instance, the quantum memory based on the laser-cooled atom usually emits at around 800 nm and a superconducting quantum processor emits microwave signal [b-Yu]. A mechanism in the QLS to convert the wavelength or encoding scheme is necessary in these scenarios.

Bibliography

[b-ITU-T X.1702] Recommendation ITU-T X.1702 (2019), *Quantum noise random number generator architecture.*

[b-IEEE P3652.1] IEEE P3652.1/D6.1 (2020), *Draft Guide for Architectural Framework and Application of Federated Machine Learning*.

[b-3GPP] 3GPP TS 36.104 (2019), LTE; *Evolved Universal Terrestrial Radio Access (E-UTRA); Base Station (BS) radio transmission and reception*.

[b-Alizadeh-1] Alizadeh, M., Yang, S., Sharif, M., Katti, S., McKeown, N., Prabhakar, B. and Shenker, S. (2013), *pfabric: Minimal Near-Optimal Data Center Transport*. In Proceedings of the ACM Special Interest Group on Data Communications Conference (SIGCOMM'13), August 12-16, Hong Kong, China.

[b-Alizadeh-2] Alizadeh, M., Greenberg, A., Maltz, D. A., Padhye, J., Patel, P., Prabhakar, B., Sengupta, S. and Sridharan, M. (2010), *Data Center TCP (DCTCP)*. ACM SIGCOMM Computer Communication Review, Vol. 40, No. 4, pp. 63–74.

[b-Altman] Altman, E., Brown, K. R., Carleo, G., Carr, L. D., Demler, E., Chin, C., DeMarco, B., Economou, S. E., Eriksson, M. A., Fu, K.-M. C., Greiner, M., Hazzard, K. R. A., Hulet, R. G., Kollár, A. J., Lev, B. L., Lukin, M. D., Ma, R., Mi, X., Misra, S., Monroe, C., Murch, K., Nazario, Z., Ni, K.-K., Potter, A. C., Roushan, P., Saffman, M., Schleier-Smith, M., Siddiqi, I., Simmonds, R., Singh, M., Spielman, I. B., Temme, K., Weiss, D. S., Vučković, J., Vuletić, V., Ye, J., Zwierlein, M. (2019), *Quantum Simulators: Architectures and Opportunities*. PRX Quantum, Vol. 2, No. 1.

[b-Amiri] Amiri, R. and Andersson, E. (2015), *Unconditionally Secure Quantum Signatures*, Entropy, Vol. 17, No. 18, pp. 5635-5659.

[b-Arute] Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., Boixo, S., Broughton, M., Buckley, B. B., Buell, D. A., Burkett, B., Bushnell, N., Chen, Y., Chen, Z., Chiaro, B., Collins, R., Courtney, W., Demura, S., Dunsworth, A., Farhi, E., Fowler, A., Foxen, B., Gidney, C., Giustina, M., Graff, R., Habegger, S., Harrigan, M. P., Ho, A., Hong, S., Huang, T., Huggins, W. J., Ioffe, L., Isakov, S. V., Jeffrey, E., Jiang, Z., Jones, C., Kafri, D., Kechedzhi, K., Kelly, J., Kim, S., Klimov, P. V., Korotkov, A., Kostritsa, F., Landhuis, D., Laptev, P., Lindmark, M., Lucero, E., Martin, O., Martinis, J. M., McClean, J. R., McEwen, M., Megrant, A., Mi, X., Mohseni, M., Mruczkiewicz, W., Mutus, J., Naaman, O., Neeley, M., Neill, C., Neven, H., Niu, M. Y., O'Brien, T. E., Ostby, E., Petukhov, A., Putterman, H., Quintana, C., Roushan, P., Rubin, N. C., Sank, D., Satzinger, K. J., Smelyanskiy, V., Strain, D., Sung, K. J., Szalay, M., Takeshita, T. Y., Vainsencher, A., White, T., Wiebe, N., Yao, Z. J., Yeh, P. and Zalcman, A. (2020). *Hartree-Fock on a superconducting qubit quantum computer*. Science, Vol. 369, No. 6507, pp. 1084–1089.

[b-Azuma] Azuma, K., Tamaki, K. and Lo, H.-K. (2015), *All-photonic quantum repeaters*. Nature Communications Vol. 6, No. 6787.

[b-BIPM-1] BIPM (2019), *The International System of Units (SI) Brochure: Unit of time (second)* [b-BIPM-2] BIPM (2017), *Recommended Values of Standard Frequencies for Applications including the Practical Realization of the Metre and Secondary Representations of the Definition of the Second: Rubidium 87 Atom*

[b-BIPM-3] BIPM (2017), *Recommended Values of Standard Frequencies for Applications including the Practical Realization of the Metre and Secondary Representations of the Definition of the Second: Strontium 87 Atom*

[b-Cheng] Cheng, P., Ren, F., Shu, R. and Lin, C. (2014), *Catch the Whole Lot in an Action: Rapid Precise Packet Loss Notification in Data Center*. In Proceedings of the 11th USENIX Symposium on Networked Systems Design and Implementation (NSDI '14), April 2–4, 2014, Seattle, WA, USA.

[b-Dupays] Dupays, A., Beswick, A., Lepetit, B., Rizzo, C. and Bakalov, D. (2003), *Proton Zemach radius from measurements of the hyperfine splitting of hydrogen and muonic Hydrogen*. Physical Review A, Vol. 68, No. 5, p. 052503.

[b-Ebubechukwu] Ebubechukwu, O. I., Tessler, L., Dowling, J. P. and Byrnes, T. (2018), *Remote quantum clock synchronization without synchronized clocks*. npj Quantum Information, Vol. 4, No. 40.

[b-Essen] Essen, L., Donaldson, R. W., Hope, E. G. and Bangham, M. J. (1973), *Hydrogen Maser Work at the National Physical Laboratory*. Metrologia, Vol. 9, No. 3, pp. 128–137.

[b-FCC] FCC Report (2019), *FCC Opens Spectrum Horizons for New Services and Technologies*. FCC Docket 18-21.

[b-Gavinsky] Gavinsky, D. (2012), *Quantum money with classical verification*. In Proceedings of the IEEE 27th Conference on Computational Complexity.

[b-Gottesman] Gottesman D. and Chuang I. (2001), *Quantum Digital Signature*, arXiv preprint quant- ph/0105032.

[b-Giovannetti-1] Giovannetti, V., Lloyd, S. and Maccone, L. (2001), *Quantum-enhanced positioning and clock synchronization*. Nature, Vol. 412, pp. 417-419.

[b-Giovannetti-2] Giovannetti, V., Lloyd, S. and Maccone, L. (2001), *Clock synchronization with dispersion cancellation*. Physical Review Letters, Vol. 87, No. 11, p. 117902.

[b-Giovannetti-3] Giovannetti V., Lloyd S., Maccone L., Shapiro, J. H. and Wong, F. N. C. (2004), *Conveyor-belt clock synchronization*. Physical Review A, Vol. 70, No. 4, pp. 1-8.

[b-Häner] Häner, T. and Steiger. D. S. (2017), *0.5 petabyte simulation of a 45-qubit quantum circuit*. In Proceedings of the International Conference for High Performance Computing, Networking, Storage and Analysis (SC '17). Association for Computing Machinery, New York, USA, No. 33, pp. 1-10.

[b-Hong] Hong C. K., Ou. Z. Y. and Mandel L. (1987), *Measurement of subpicosecond time intervals between two photons by interference*. Physical Review Letters, Vol. 59, No. 18, pp. 2044-2046.

[b-Huitema] Huitema, C. (2003), *Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP).* RFC 3605.

[b-Kandala-1] Kandala, A., Mezzacapo, A., Temme, K., Takita, M., Brink, M., Chow, J. M., and Gambetta, J. M. (2017). *Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets*. Nature, Vol. 549, pp. 242–246.

[b-Kandala-2] Kandala, A., Temme, K., Córcoles, A. D., Mezzacapo, A., Chow, J. M., and Gambetta, J. M. (2019), *Error mitigation extends the computational reach of a noisy quantum processor*. Nature, Vol. 567, No. 7749, pp. 491–495.

[b-Kómár] Kómár, P., Kessler, E. M., Bishof, M., Jiang, L., Sørensen, A. S., Ye, J. and Lukin, M. D. (2014), *A quantum network of clocks*. Nature Physics, Vol. 10, No. 8, pp. 582-587.

[b-Li] Li, Q., Chan, W. H., Wu, C. and Wen, Z. (2014), *Triple-server blind quantum computation using entanglement swapping*. Physical Review A, Vol. 89, No. 4, pp. 2748-2753

[b-Lipinska] Lipinska, V., Murta, D. and Wehner, S. (2018), *Anonymous transmission in a noisy quantum network using the W state*, Physical Review A, Vol. 98, No. 1052320.

[b-Lo] Lo, H.-K. and Chau, H. F. (1997), *Is Quantum Bit Commitment Really Possible?* Physics Review Letters, Vol. 78, No. 13410.

[b-Mao] Mao, Y., Wang, B. X., Zhao, C., Wang, G., Wang, R., Wang, H., Zhou, F., Nie, J., Chen, Q., Zhao, Y., Zhang, Q., Zhang, J., Chen, T.-Y. and Pan, J.-W. (2018), *Integrating quantum key distribution with classical communications in backbone fiber network*. Optics Express, Vol. 26, No. 5, pp. 6010-6020.

[b-Meraner] Meraner, M, Mazloom, A., Krutyanskiy, V., Krcmarsky, V., Schupp, J., Fioretto, D. A., Sekatski, P., Northup, T. E., Sangouard, N. and Lanyon, B. P. (2020), *Indistinguishable photons from a trapped-ion quantum network node*. Physical Review A Vol. 102, No. 5.

[b-Mirhosseini] Mirhosseini, M., Magaña-Loaiza, O. S., O'Sullivan, M. N., Rodenburg, B., Malik, M., Lavery, M. P. J., Padgett, M. J., Gauthier, D. J., and Boyd, R. W. (2015), *High-dimensional quantum cryptography with twisted light*. New Journal of Physics, Vol. 17, No. 3, p. 033033.

[b-Morimae-1] Morimae, T. and Fujii, K. (2012), *Blind Quantum computation protocol in which Alice only makes measurements*. Physical Review A, Vol. 87, No. 5.

[b-Morimae-2] Morimae, T. and Fujii, K. (2013), *Secure entanglement distillation for double-server blind quantum computations*. Physical Review Letters Vol.111, No. 2, pp. 47-89.

[b-NIST-1] NIST news (2006), *Mercury Atomic Clock Keeps Time with Record Accuracy*.

[b-NIST-2] NIST news (2008), NIST 'Quantum Logic Clock' Rivals Mercury Ion as World's Most Accurate Clock.

[b-Peruzzo] Peruzzo, A., McClean, J., Shadbolt, P., Yung, M.-H. H., Zhou, X.-Q. Q., Love, P. J., Aspuru-Guzik, A., and O'Brien, J. L. (2014). *A variational eigenvalue solver on a photonic quantum processor*. Nature Communications, Vol. 5, No. 4213.

[b-QIT4N D1.1] ITU-T Technical Report (2021), *Quantum information technology for networks terminology: Network aspects of quantum information technologies*

[b-Sheng] Sheng, Y. B. and Zhou, L. (2015), *Deterministic entanglement distillation for double-server blind quantum computations*. Scientific Reports, Vol. 5, No. 7815.

[b-Unnikrishnan] Unnikrishnan, A., MacFarlane, I. J., Yi, R., Diamanti, E., Markham, D. and Kerenidis, I. (2019), *Anonymity for Practical Quantum Networks,* Physics Review Letters, Vol. 122, No. 1240501.

[b-Valencia] Valencia A., Scarcelli, G. and Shih, Y. H. (2004), *Distant clock synchronization using entangled photon pairs*. Applied Physics Letters, Vol. 85, No. 13, pp. 2655-2657.

[b-Wehner] Wehner, S., Elkouss, D. and Hanson, R. (2018), *Quantum internet: A vision for the road ahead*, Science, Vol. 362, No. 16412.

[b-Wiesner] Wiesner, S. (1983), *Conjugate coding*. SIGACT News, Vol. 15, No. 1, pp. 78-88.

[b-Xavier] Xavier, G. B., Walenta, N., Vilela de Faria, G., Temporão, G. P., Gisin, N., Zbinden, H. and von der Weid, J. O. (2009), *Experimental polarization encoded quantum key distribution over optical fibres with real-time continuous birefringence compensation*. New Journal of Physics Vol. 11, No. 4, p. 045015.

[b-Xia] Xia, J., Zeng, G., Zhang, J., Wang, W., Bai, W., Jiang, J. and Chen, K. (2019), *Rethinking Transport Layer Design for distributed machine learning*. In Proceedings of the 3rd Asia-Pacific Workshop on Networking (APNet '19), August 17–18, Beijing, China.

[b-Xie] Xie, D., Peng, J., Zhao, J. and Huang H. (2011), *Theoretically Exploring a Better way of Quantum Clock Synchronization Using MZ (Math-Zehnder) interferometer*. Journal of Northwestern Polytechnical University, Vol. 29, No. 4.

[b-Yu] Yu, Y., Ma, F., Luo, X.-Y., Jing, B., Sun, P.-F., Fang, R.-Z., Yang, C.-W., Liu, H., Zheng, M.-Y., Xie, X.-P., Zhang, W.-J., You, L.-X., Wang, Z., Chen, T.-Y., Zhang, Q., Bao, X.-H. and Pan, J.-W. (2020), *Entanglement of two quantum memories via fibres over dozens of kilometres*. Nature Vol. 578, No. 7794, pp. 240–245.