2020·广州
世界5G大会
WORLD 5G CONVENTION

PRELIMINARY STUDY OF ADVANCED TECHNOLOGIES TOWARDS 6G ERA: QITS 2020

WHITE PAPER V7.0 F
2020.11

Preliminary Study of Advanced Technologies towards 6G Era: QITs

2020

Executive Summary

The year of 2020 not only marks the first year of a large-scale commercial deployment of 5G, but also witnesses a worldwide pandemic of the third zoonotic human coronavirus of the century, namely the COVID-19. The COVID-19 imposes great impact on all aspects of our society, such as the way people live, work, socialize, travel, and so on. In particular, the consequent change of underlying pattern in information demand is calling for a revolutionary promotion in information processing capability in order to speed up the growth of a new society in 6G era characterized by pervasive digitization, ubiquitous connection and high-level intelligence.

The vision of quantum information technologies (QITs) is to provide a radically new information processing paradigm by exploiting quantum mechanics. Being in synergy with existing information systems in the classical domain, QITs are anticipated to achieve unparalleled capability of information processing, which is entailed by the era of 6G and beyond, to endow people with safer and smoother lives and to enable society with ever-increasing productivity.

The rapidly developing QITs, including quantum communication, computing, and sensing & metrology, will impose profound impacts on information and communication technology (ICT), and finally, forge the so-called “quantum internet”. This white paper gives an overview of QITs in the first part. It will firstly outline the various QITs and their potential impact on ICT networks. Then, it will introduce the concept of quantum internet, and try to take a closer look at it from the perspectives of both application and technology evolution. Moreover, the quantum network related standardization activities will also be summarized. Finally, we will illustrate the possible implications for 6G with the development of a quantum internet.

As with any interdisciplinary field, developing and applying QITs requires sustained coordination among all involved disciplines mainly of physics, computer science, and information theory. From the perspectives of 6G system design, it is critical to know about the underlying connection between QITs and emerging communication technologies. Therefore, in the second part, this white paper provides insights into how QITs can be applied in boosting communication performance by employing two instances related to non-orthogonal multiple access (NOMA) and polar code, respectively.

Table of Contents

1 Introduction

The scope of this annually revised white paper is to introduce quantum information technologies (QITs) with the aim of taking advantages of their powerful information processing capabilities to fulfil stringent demands of communication and computing envisaged by 6G systems. Our previous version in 2019 briefly introduced overview of QITs and preliminary knowledges of quantum communication as well as quantum computing. In particular, in the quantum computing part, major contributions of quantum multi-user detection (Q-MUD) were discussed classifiedly. The version of 2020 will further elaborate the state-of-the-art in the QITs area from the following two aspects.

Chapter 2. QITs and Quantum Internet

The rapidly developing QITs, including quantum communication, computing, and sensing & metrology, will impose profound impacts on the ICT, and finally, forge the so-called “quantum internet”. This chapter will firstly outline the various QITs and their potential impact on ICT networks. Then, it will introduce the concept of quantum internet, and try to take a closer look at it from the perspectives of both application and technology evolution. Moreover, the quantum network related standardization activities will also be summarized. Finally, we will illustrate the possible implications for 6G with the development of quantum internet.

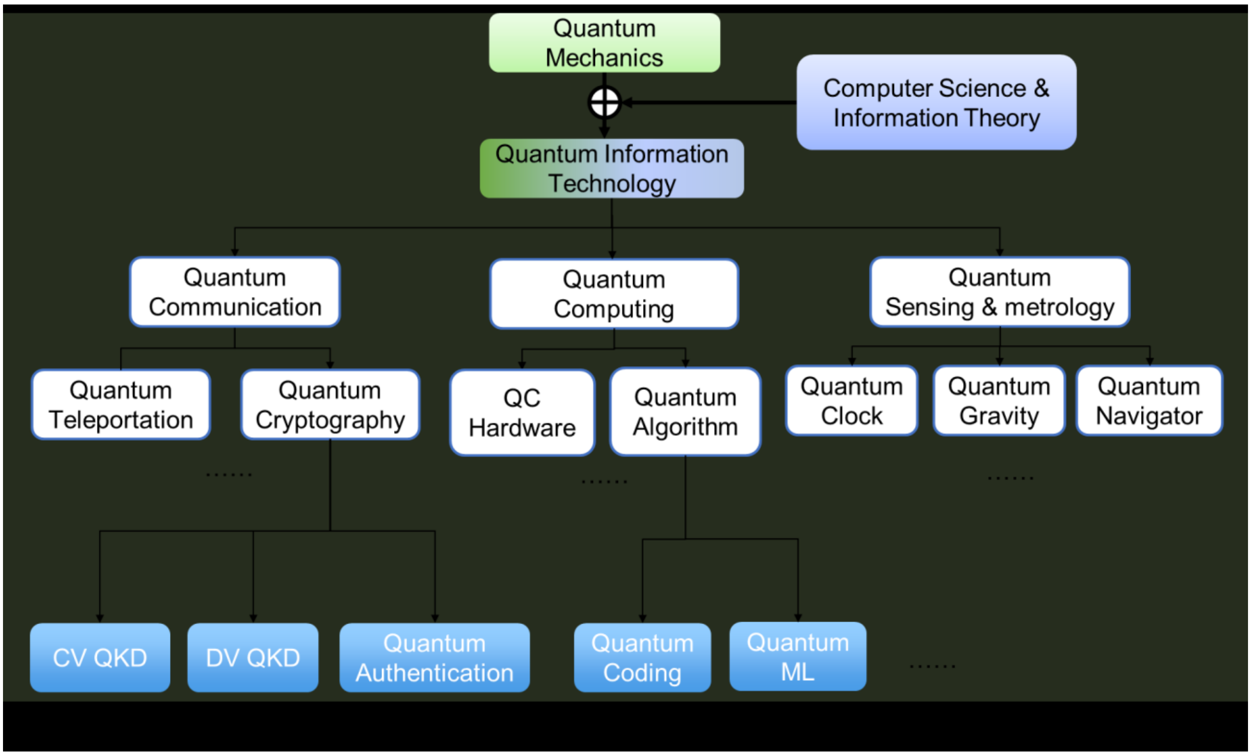
Chapter 3. QTIs for Classical Signal Processing

This chapter employs two instances to illustrate how QITs can be applied in boosting communication performance. The first instance introduces Q-MUD for sparse code multiple access (SCMA), which as one non-orthogonal multiple access (NOMA) scheme has been proved to overcome the scarcity of resources by providing high spectral efficiency gain at the cost of a high-complexity multi-user detection (MUD). The Q-MUD of SCMA provides insights into how to exploit quantum computing in reducing high complexity suffered by classical decoder. The second instance introduces polar code, which is capable of approaching Shannon’s capacity at a low encoding and decoding complexity. However, the data dependencies in the decoding process result in high decoding latency. This instance tries to exploit the inherent parallel due to the quantum superposition by identifying isomorphism between the classical and quantum paradigms for polar code.

2 QITs and Quantum Internet

2.1 Overview of QITs

Quantum information technology (QIT) is a class of emerging technologies that improves the information processing capability by harnessing principles of quantum mechanics. The rapidly developing quantum information technologies, including quantum communication, computing, and sensing & metrology, have promoted the booming of the second quantum revolution and will have a profound impact on ICT networks. We will briefly introduce the following main QIT concepts (as structured in Figure 2.1) and their potential impacts (as illustrated in Figure 2.2).



Figuure 2.1 Concepts of QITs

- **Quantum Communication**

Quantum communication includes a class of novel communication technologies that exploit the transmission of quantum signals, such as quantum key distribution (QKD), quantum teleportation, quantum repeater and etc. QKD is one of the most mature QIT applications at the moment. Different from the traditional key distribution technology, QKD provides long-term security based on principles of quantum mechanics. The security of QKD still holds even under the attack of unbounded computation power, which includes quantum computer. Metropolitan and backbone QKD networks have been constructed worldwide, satellite-based quantum communication experimental applications have been realized in last decade. In the future, quantum repeater would be an essential building block in constructing distributed quantum computing.

- **Quantum Computing**

Quantum computing is a new computation model that follows the laws of quantum mechanics to control quantum information units. Combined with the quantum parallelism, quantum information processing has greater potential than classical information processing. Quantum computers represent a breakthrough in Moore's Law that is limited by the nanoscale, implying enormous computing power potential. Quantum computer has potential applications in many fields, such as optimization over huge data sets and design of new materials and molecular functions. The computational power brought by quantum computing will not only improve the performance of signal processing, but also become a threat to security of existing ICT networks.

- **Quantum Metrology**

Quantum metrology is the study of measurement techniques that gives higher resolutions and sensibilities in measurements of physical parameters than the similar measurement performed in a classical framework. At this stage, quantum metrology is mainly used in the fields of navigation, lidar and time-frequency transmission.

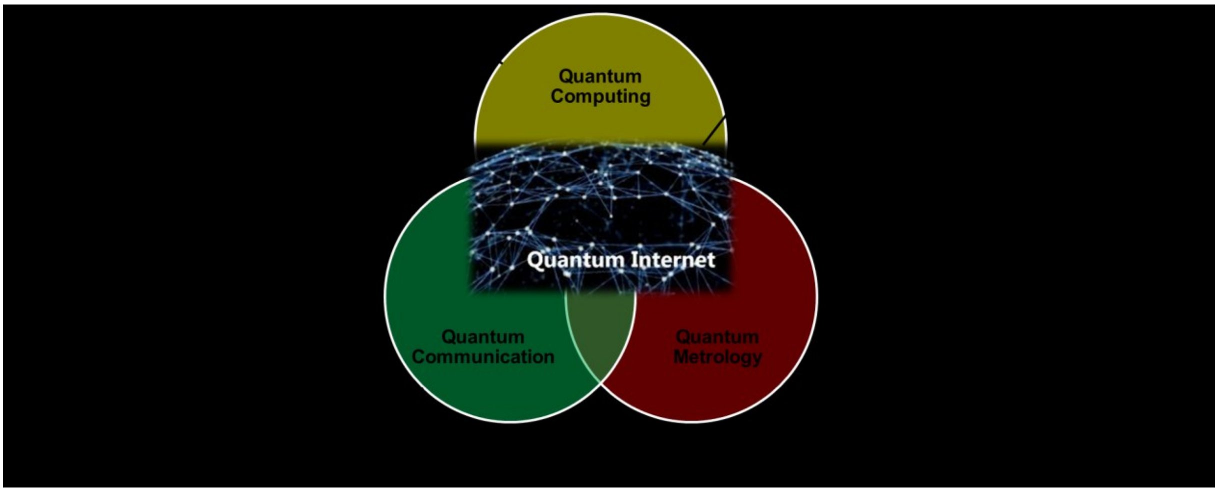


Figure 2.2 The Potential Impact of QITs

In the last decade, the development of QIT research and application have been accelerated globally. QIT has become the center of focus not only in academia, but also in industry and standardization communities. QKD-based secure communication networks have been/are being built in many countries [1][2]. Quantum teleportation based 'quantum internet' project has been initiated in EU quantum flagship [3]. Satellite based wide-area quantum communication experiments have been reported [4]. Different kinds of quantum computer prototypes, including superconductive circuits, trapped ions and semiconductor have been demonstrated. Quantum-based clock, gravimeter, magnetometer and gyroscope have been extensively investigated.

2.2 QITs Evolution towards Quantum Internet

2.2.1 What is Quantum Internet?

With the fast development of QITs, it will not only have significant impacts on ICT networks, but also bring new forms of network, i.e., quantum information network (QIN), which also can be called as "quantum internet". The QIN is expected to connect quantum information processing nodes, including QKD nodes, quantum computers and quantum sensors, via quantum communication technologies such as quantum teleportation and quantum repeating, to realize full quantum information transmission and networking. QIN has potentials to provide series of new applications, such as distributed quantum computing and quantum sensor network.

The concept of "Quantum Internet" was firstly proposed by Kimble in 2008 [5]. The basic idea was "to create a quantum network, quantum information is generated, processed, and stored locally in quantum nodes. These nodes are linked by quantum channels that transport quantum states from site to site with high fidelity and that distribute entanglement across the entire network." Recent years, Quantum Internet has become a hot topic and strategic goal for global "Quantum Race".

The USA White House's National Quantum Coordination Office has released "A STRATEGIC VISION FOR AMERICA'S QUANTUM NETWORKS" report in February 2020 [6]. It says: ***"Exploring how to build the quantum internet—a vast network of quantum computers and other quantum devices—will catalyze new technologies that accelerate today's internet, improve the security of our communications, and allow dramatic advances in computing."***

The European Commission has released the report of "Strategic Research Plan for Quantum Flagship Projects" in March 2020 [3]. It mentioned: ***"The long-term vision is to realize a Quantum Internet; quantum computers,***

simulators, and sensors, interconnected via quantum networks distributing information and quantum resources such as coherence and entanglement, to provide European citizens with more secure telecommunications and data storage, improved healthcare, and better performing computation."

2.2.2 Evolution from Application Perspective

With the development of quantum information technologies, quantum networks and applications will continue to evolve. As presented in the research report "Opportunities in the Quantum Era" released by the UK's Office of Science in 2016 [7], the development trend of quantum communication applications was described as shown in Figure 2.3. It indicates that quantum communication applications at this stage are mainly in the security applications of quantum random numbers, QKD link encryptions and other technologies in the fields of government affairs, national defense, and data centers; in the future, as QKD networking becomes mature, and end equipment tends to miniaturization and mobilization, it will also extend to wider application areas such as telecommunications networks, enterprise networks, consumers, and cloud storage; in the long run, with the development of technologies such as quantum satellites, quantum relays, quantum computing, and quantum sensing, the breakthrough will also produce a series of new applications such as quantum cloud computing and distributed quantum sensing.

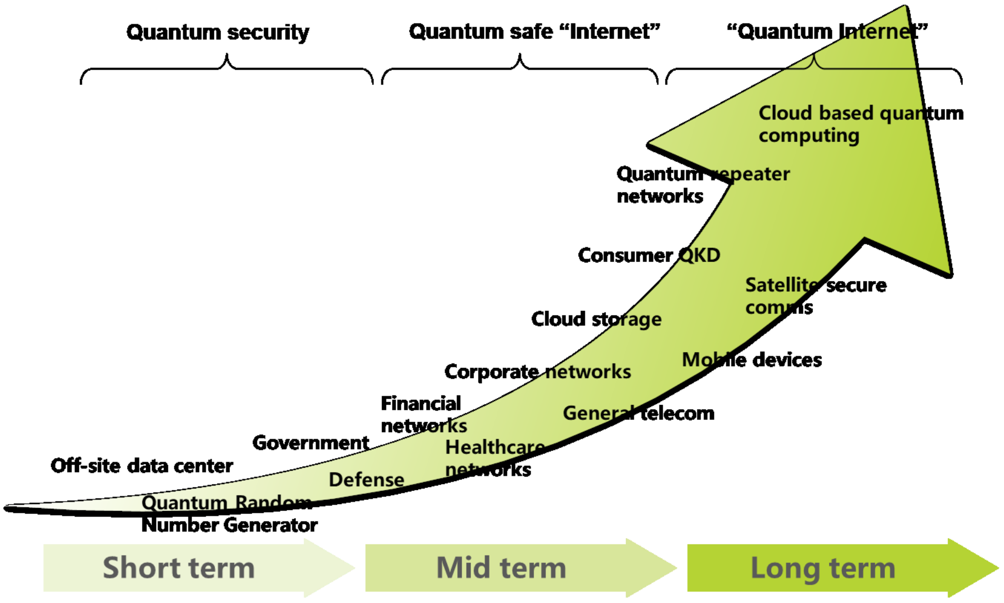


Figure 2.3 Development of Quantum Communication Applications [7]

Based on this blueprint and the current development trend of quantum technology, the development of quantum communication networks and applications can be roughly divided into three stages:

- The first stage is the current quantum key distribution network based on the combination of point-to-point link QKD technology and classical communication and cryptography technologies such as trusted relay and symmetric cryptography, mainly for high security applications in special domain such as finance, government affairs, to provide high-level confidential communication services in demand scenarios;
- The second stage is based on the breakthrough of chip-based and mobile QKD technology to achieve a quantum secure Internet that integrates QKD with existing Internet terminals and services. It can provide quantum security services to a wide range of fields, e.g., telecommunications, enterprises, consumers, and cloud services;
- The third stage is based on breakthroughs in quantum relay, quantum memory, and quantum computing technologies. Quantum computing processors and quantum sensors are interconnected through a quantum communication network that can transmit qubits over long distances to form a quantum network carrying quantum information. The so-called Quantum Internet can provide new services such as quantum cloud computing, distributed quantum sensing, quantum secure communications, quantum clock synchronization, quantum telescopes, and quantum gravitational wave detection [8].

2.2.3 Evolution from Technology Development Perspective

In July 2020, the U.S. **Department of Energy (DOE)** released a report on the blueprint for the development of the quantum Internet [6]. The goal is to build a second Internet parallel to the existing Internet——the quantum Internet, to support the smooth implementation of the National Quantum Initiative Act and to ensure that the United States is at the forefront of the global quantum race.

The report pointed out that the quantum Internet is a new type of Internet that uses the principles of quantum mechanics to ensure the secure transmission of information and connects a new generation of quantum computers and quantum sensors, which can also coexist with existing Internet networks. The report illustrated the five key milestones for the deployment of the quantum internet as shown in Figure 2.4:

(1) **Verification of Secure Quantum Protocols over Fiber Networks:** to achieve a prepare and measure quantum network connected via trusted nodes, and further realize the programmable classic-quantum network

based on SDN control. An application domain of interest is the protection of critical infrastructures through secure communication based on quantum key distribution e.g., within the electrical power grid;

(2) **Inter-campus and Intra-city Entanglement Distribution:** to achieve metropolitan area networking that realizes quantum entanglement distribution based on optical switch, and then realizes small-scale quantum sensor network applications;

(3) **Intercity Quantum Communication using Entanglement Swapping:** to develop quantum memory network, in which any two end users (nodes) can obtain and store entangled qubits and teleport quantum information to each other, and to realize the inter-city long-distance quantum communication network;

(4) **Interstate Quantum Entanglement Distribution using Quantum Repeaters**: In this stage, classic and quantum networking technologies have been integrated. Successful concatenation of quantum repeaters and quantum error-corrected communication with respect to loss and operational errors over continental-scale distances will pave the way for operational entanglement distribution networks covering longer distances, enabling a quantum Internet to be created.;

(5) **Build a Multi-institutional Ecosystem between Laboratories, Academia, and Industry to Transition from Demonstration to Operational Infrastructure:** to realize the transition from the demonstration of quantum Internet to the commercial operational infrastructure, to construct the multi-institutional ecosystem across academia, national quantum laboratories, and industry, to develop a "quantum-smart" workforce, to achieve the coordinated development of ground and satellite quantum networks, and the practical application of quantum communications.

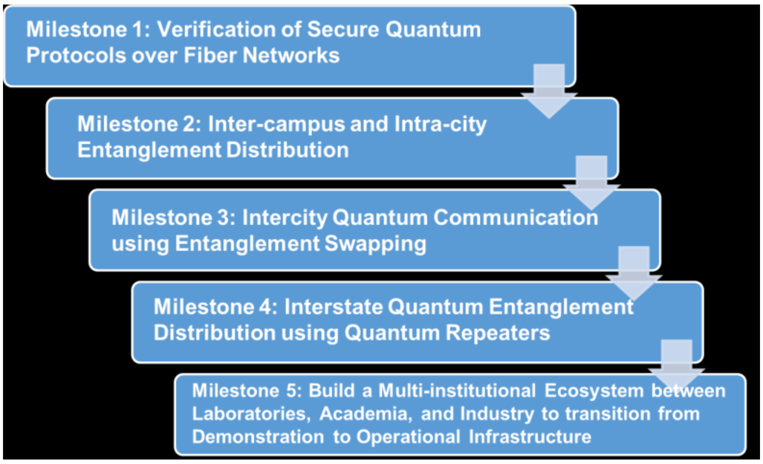


Figure 2.4 Key Milestones towards Quantum Internet [6]

Similarly, researchers from Delft share their own vison on the Quantum Internet： fundamentally enhance internet technology by enabling quantum communication between any two points [13]. Regarding to the technology developments, they have identified the essential quantum components required for the quantum internet, which are quantum channels, quantum repeaters and quantum processors, Five technological development stages towards the Quantum Internet have been also proposed. Practically, from the initial to the final form, the stages of quantum internet are trusted repeater networks, prepare and measure networks, entanglement distribution networks, quantum memory networks, fault-tolerant few-qubit networks and quantum memory networks.

2.3 Standardization Activities

This chapter will introduce the ongoing standard developing organization (SDO) activities for QIT including ISO/IEC JTC1, ITU-T, IETF, IEEE, ETSI, etc. The current standardization activities for quantum information technologies for networks can be briefly categorized into the following three major subjects, referring to Figure 2.5.

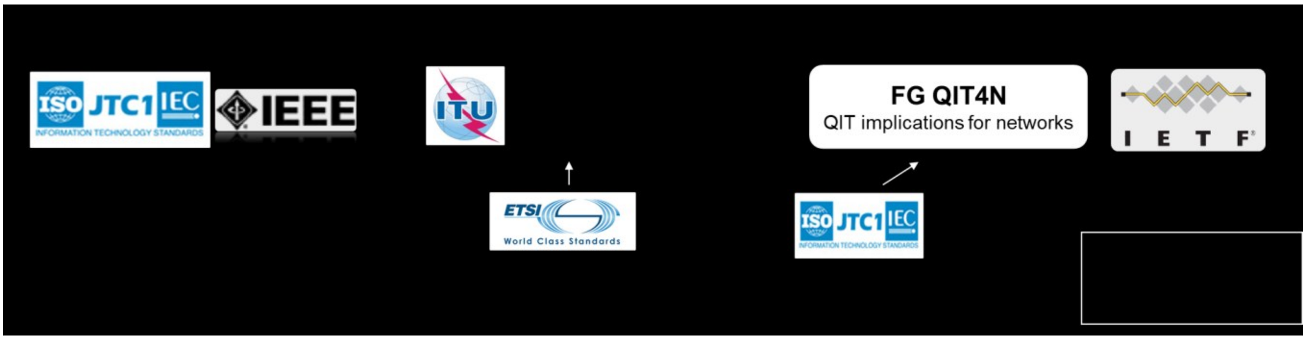


Figure 2.5 QIT related SDO Activities

(1) Quantum Computing

In 2018, ISO/IEC JTC1 established two study groups, i.e., SG2 and SC7/SG1 on Quantum Computing. In 2019, ISO/IEC JTC1 reconstituted an Advisory Group (AG) on Quantum Computing after the term ‘study group’ was abandoned in ISO/IEC JTC1. In 2020, JTC1 established the WG14 to take the lead in formulating international standards such as quantum computing terminology.

In 2018, IEEE initiated two work items on Quantum Computing Definition (P7130) and Performance Metrics & Benchmarking (P7131). In June 2019, IEEE revised P7130 into Standard for Quantum Technologies Definitions, providing a general nomenclature for Quantum technology.

The standardization on quantum computing is still at a very initial stage, mainly aims to clarify concepts, define terminologies, identify standardization needs and provide performance metrics & benchmarking.

(2) Quantum Communication

Quantum key distribution, as one of the most mature applications of quantum communication in ICT networks, has induced a series of standardization activities in ETSI, ISO/IEC JTC 1 and ITU-T. ETSI initiated the industry specification group (ISG) on QKD in 2008. ETSI ISG-QKD has published 9 specifications on QKD until 2019 and have several work items ongoing. ITU-T SG13 and SG17 have initiated 12 work items on QKD network functional aspects, and 6 work items on QKD network security aspects, with two Recommendations Y.3800 and X.1702 published. ISO/IEC JTC 1/SC 27 initiated the study period "Security requirements, test and evaluation methods for quantum key distribution" in 2017. In 2019, the study period was finished and the work item for ISO/IEC 23837 (Part 1&2) was established.

Besides QKD, IEEE has initiated P1913 - Software-Defined Quantum Communication in 2016, which aims to define the Software-Defined Quantum Communication protocol that enables configuration of quantum endpoints in a communication network in order to dynamically create, modify or remove quantum protocols or applications.

(3) Quantum Internet

In 2018, IRTF established the "Quantum Internet Research Group (QIRG)". QIRG aims to study the evolution from a QKD network based on trusted relay to a quantum Internet, which composed of quantum relay, quantum computing, and quantum storage. They have developed 6 drafts, and currently the documents on quantum internet architectural principles and use cases are still under preparation. In addition, QIRG also released the Quantum Internet Software Simulator (SimulaQron) for protocol research and security assessment, and organized a hackathon for the Quantum Internet.

In 2019, ITU-T established the focus group on Quantum Information Technology for Networks (FG-QIT4N), which is envisioned to be an open platform for global interested stakeholders to share knowledge, best practices and lessons learned to take full advantage of the ability and potential of QIT in networks. The FG-QIT4N is led by three co-chairmen from USA, Russia and China (Prof. Zhang Qiang from USTC). It has set up two branches of work groups with 9 reports to be delivered: 1) WG1 is for network aspects of QIT, which is to study the evolution of QIT and QIN beyond QKD, led by Mr. Helmut Griesser, Germany; 2) WG2 is for QKD network, led by Mr. Zhangchao Ma, China.

2.4 Implications for 6G

This chapter wil discuss the implications of quantum networks for the future 6G technology. The relationship of quantum network and 6G network can be illustrated as Figure 2.6. The future 6G can provide key network infrastructure for the quantum and classical channel requirements to construct a quantum network. The potential impact and benefits brought by QITs will include security enhancement, precision time synchronization, boosting signal and data processing capabilities, etc.

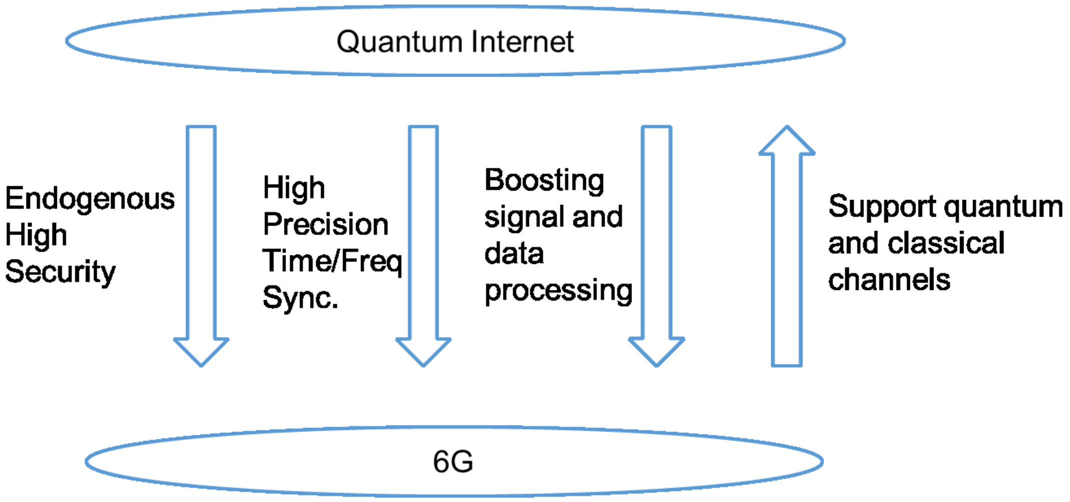
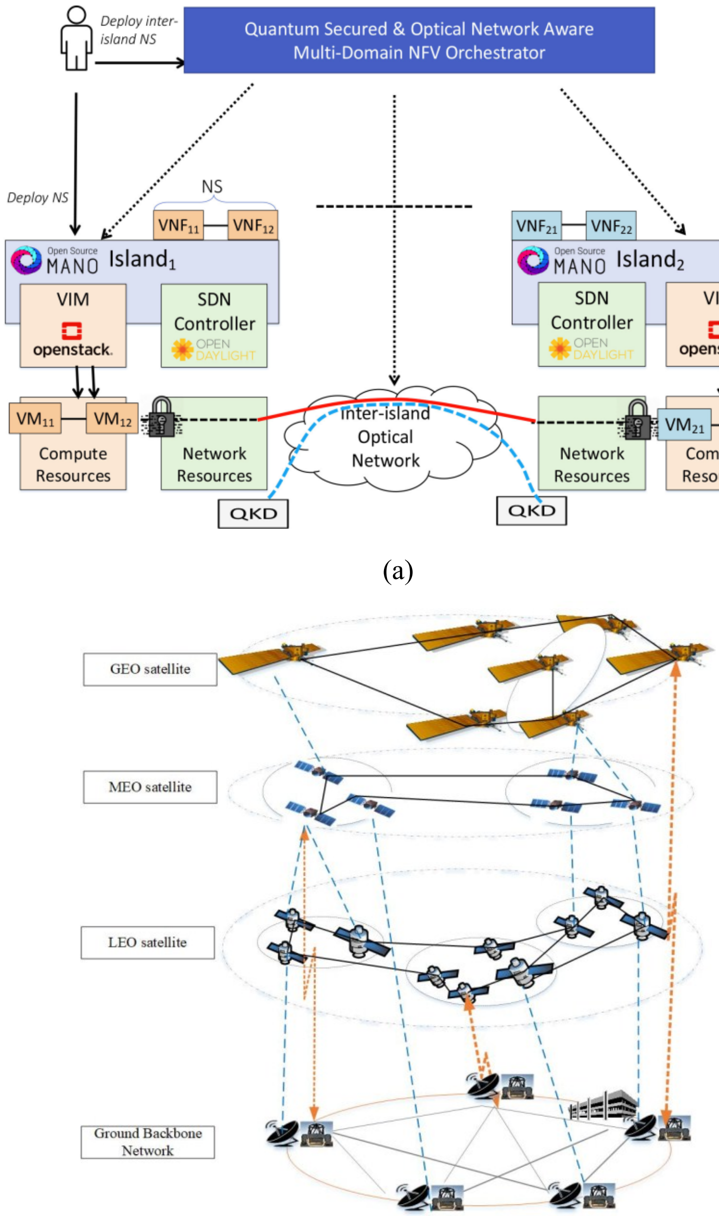


Figure 2.6 Implications of quantum internet for 6G

2.4.1 Quantum-based Security Enhancement

At present, the most mature application for QITs are QKD and quantum random number generation (QRNG). Integration of QITs with 5G and future communication networks for security enhancement has become a hot topic. The scientific research institutions and telecom operators in Europe, South Korea and other places attach great importance to the development of quantum safe communication technologies, and actively practicing the integration of QITs into the 4G/5G network to enhance network security [8][10].

In 2019, the British Quantum Communication Hub and Bristol University carried out a series of 5G+QKD fusion technology research, and held a live network demonstration conference on September 2019 [11], which combined SDN and QKD in the 5G network. New technologies such as NFV and AI are combined with QKD to realize quantum-secure multi-domain NFV orchestrator in the 5G test network, as well as security enhancement applications such as QKD-based Inter-DC data secure transmission, as shown in Figure 2.7(a). In future, quantum security schemes will also play an important role in securing the inter-satellite and satellite-ground communication network as envisioned in 6G as shown in Figure 2.7(b).



(a)

(b)

Figure 2.7 Quantum Network Applications to Enhance Security

2.4.2 Quantum-based Precision Timing and Synchronization

The new features of 5G such as high-precision positioning and high-performance network coordination have put forward higher requirements for network time-frequency synchronization. Quantum enhanced clocks and time distribution technologies are expected to greatly improve the accuracy of network time/frequency synchronization, thereby enhancing the technical performance of the new generation of telecommunication networks, which will be especially important for time-sensitive services, positioning, navigation, signal coordination, etc. An exemplary quantum network application to enhance synchronization is shown in Figure 2.8.

Figure 2.8 Quantum Network Applications to Enhance Synchronization [12]

2.4.3 Quantum Algorithms for High Performance Signal and Data Processing

With the introduction of new features such as large bandwidth, massive MIMO, and multi-point cooperation in 5G and its evolution networks, technologies such as power allocation, multi-user detection (MUD), and MIMO detection in mobile networks require massive calculations to optimize performance. Classical algorithms will become increasingly difficult to perform. Quantum algorithms based on quantum computers are expected to solve these mobile communication algorithm problems more efficiently. Quantum algorithms for specific problems in mobile networks will probably become a research hotspot in the next generation of mobile communication networks. The application of quantum algorithm for boosting signal processing performance will be detailed in Chapter 3.

3 QITs for Classical Signals Processing

As with any interdisciplinary field, developing and applying QITs requires sustained coordination among all involved disciplines mainly of physics, computer science, and information theory. From the perspectives of 6G system design, it is critical to know about the underlying connection between QITs and emerging communication technologies. Therefore, this chapter provides insights into how QITs can be applied in boosting communication performance by employing two instances related to non-orthogonal multiple access (NOMA) and polar code, respectively. One is quantum multi-user detection (Q-MUD) of sparse code multiple access (SCMA) illustrating how to exploit quantum computing in reducing high complexity suffered by classical decoder. The other tries to exploit the inherent parallel due to quantum superposition by identifying isomorphism between the classical and quantum paradigms for polar code.

3.1 Quantum SCMA Decoder

NOMA schemes are promising to overcome the scarcity of resources envisioned by next generation communication systems, while supporting massive connectivity. As one of NOMA schemes, SCMA has been proved to provide high spectral efficiency gain at the cost of a high-complexity multi-user detection (MUD). Fortunately, quantum search techniques were shown to substantially reduce the complexity of multi-user detectors. As an open problem, therefore, the quantum search-aided MUD of SCMA provides insights into how to exploit quantum computing in reducing high complexity suffered by classical decoder [14].

3.1.1 SCMA Decoder in the Classical Domain

Figure 3.1 shows a structure of uplink SCMA with Turbo coding. Assume a NOMA system, in which K $(K > 0)$ users transmit to a common Base Station (BS) simultaneously in the shared spectrum. The bit stream of the user $k \in [1..K]$ emanating from the source is denoted by b_k , which is entered into the turbo encoder. The output of the turbo encoder is divided into code blocks, where each block consists of R coded bits. A code block is denoted by $c_k = \left(c_{k,1}, c_{k,2}, \dots, c_{k,R}\right)^T$, which is forwarded to the SCMA encoder. In the SCMA encoder, c_k is mapped into an N-dimensional SCMA codeword denoted by $x_k = \left(x_{k,1}, x_{k,2}, \ldots, x_{k,N}\right)^T$ that is selected from the SCMA codebook χ_k of size $M = 2^R$. Finally, the SCMA codewords are transmitted by the Orthogonal Frequency Division Multiplexing (OFDM) modulator.

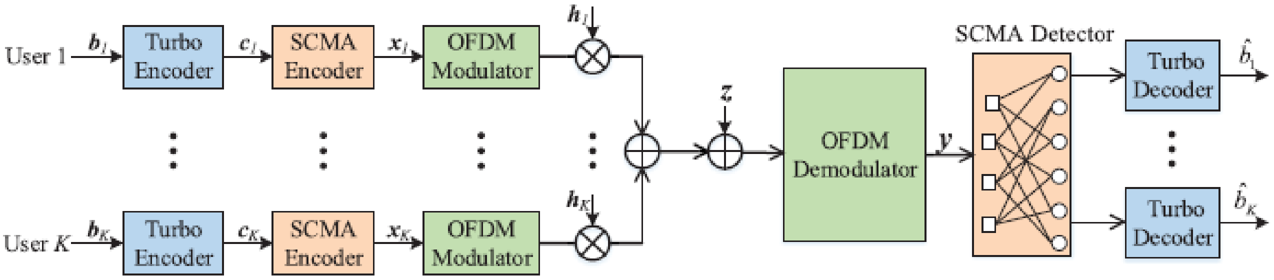
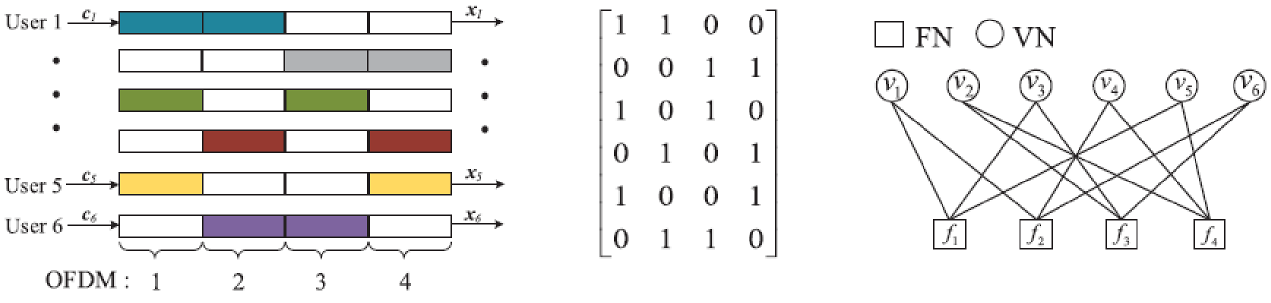


Figure 3.1 Uplink SCMA with Turbo Coding

The modulated symbols are transmitted through the wireless channels by using N OFDM sub-carriers. Let $h_{k,n}$ denote the channel coefficient of the link between the BS and user k on the n-th sub-carrier. The channel vector between user k and the BS is given by $h_k = \left(h_{k,1}, h_{k,2}, \ldots, h_{k,N}\right)^T$. In addition, let z_n denote the Additive White Gaussian Noise (AWGN) imposed on the n-th sub-carrier with variance σ^2. The noise imposed on the transmitted signal is denoted by $z = (z_1, z_2, \ldots, z_N)^T$. At the BS side, the received signal is denoted by $y = \sum_{k=1}^{K} diag\{h_k\} x_k + z$.

According to Figure 3.2, the structure of SCMA codeword is characterized by using the concepts of mapping matrix and factor graph. Figure 3.2 (a) shows that the colored blocks represent the non-zero elements in the SCMA codewords, while the blank blocks represent the zero elements. In this example, the parameters are set as K = 6 and N = 4. Figure 3.2 (b) shows the mapping matrix, denoted by F, which is a $(K \times N)$-element matrix. If the n-th element of k-th user's codeword is non-zero, then we have $F_{k,n} = 1$, otherwise $F_{k,n} = 0$. Figure 3.2 (c) shows the factor graph, denoted by $\mathcal{F}(\mathcal{V}, \mathcal{N})$, which is a bipartite graph with N function nodes (FN) and K variable nodes (VN). On the factor graph, the n-th FN is connected to the k-th VN via an edge if $F_{k,n} = 1$. Moreover, the set $\phi(\mathrm{n})$ is defined as the collection of neighboring nodes of FN n ,while the neighbor nodes of VN k are defined as $\psi(k)$. Thus, the degree of $\phi(\mathrm{n})$ and $\psi(k)$ are $d_f = 3$ and $d_v = 2$, respectively. Additionally, the sets $\phi(\mathrm{n})$ and $\psi(k)$ represent the users colliding on the n-th OFDM sub-carrier and the OFDM subcarriers used to transmit the k-th user's data, respectively.



$$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

(a) (b) (c)

Figure 3.2 The Structure of SCMA Codewords

Figure 3.3 shows the iterative structure of SCMA MUD, in which the extrinsic information is exchanged between the SCMA detector and the turbo decoder. In the SCMA detector, the *a posteriori* Log-Likelihood Ratio (LLR) is denoted by L_1 of each channel coded bit, while in the turbo decoder, the *a posteriori* LLR is denoted by L_2. $\lambda_1(c_{k,r})$ and $\lambda_2(c_{k,r})$are the extrinsic information delivered by the SCMA detector and turbo detector, respectively. $\lambda_1^P(c_{k,r})$ and $\lambda_2^P(c_{k,r})$ are the *a priori* LLR delivered by the SCMA decoder and turbo decoder, respectively. We have $L_1(c_{k,r}) = \lambda_1(c_{k,r}) + \lambda_2^P(c_{k,r})$ and $L_2(c_{k,r}) = \lambda_2(c_{k,r}) + \lambda_1^P(c_{k,r})$.

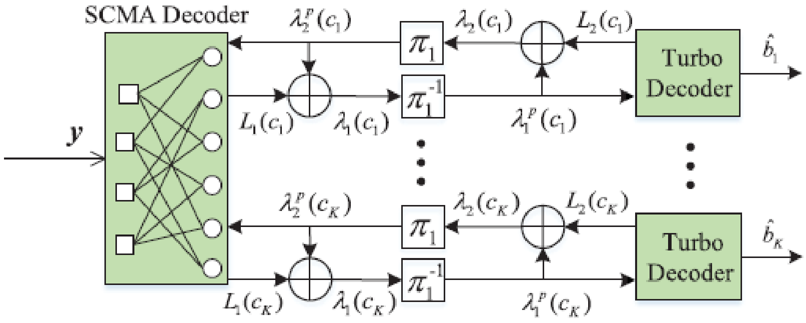


Figure 3.3 The Iterative Structure of the MUD

3.1.2 Quantum-assisted SCMA Decoder

The MUD relies on the classical Message Passing Algorithm (MPA) based detector that achieves near-optimal Bit Error Rate (BER) performance. However, the classical MPA exhibits an exponentially growing complexity with the number of users. Therefore, Quantum-assisted MPA (Q-MPA) based iterative MUD is introduced by using Durr-Hoyer Quantum Search Algorithm (DH-QSA) [15] to reduce the complexity of the classical MPA. Using the

Q-MPA, we can obtain the value of $\lambda_1(c_{k,r})$ in the SCMA detector at the cost of a reduced number of cost-function (CF) evaluations.

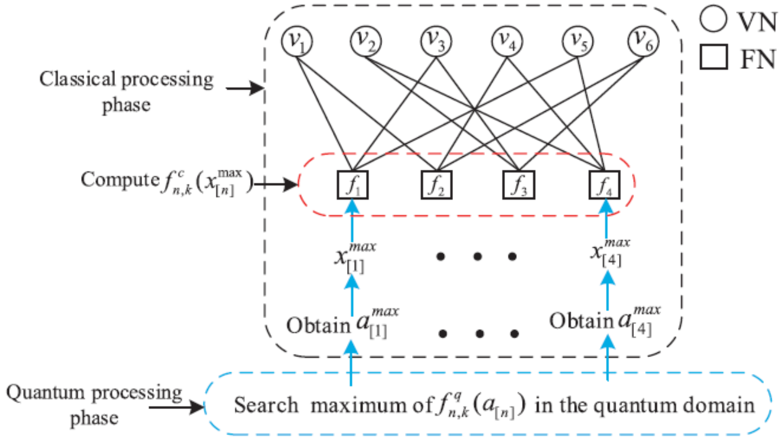


Figure 3.4 The Diagram of Q-MPA

Figure 3.4 shows the diagram of Q-MPA, which consists of message updating in FNs, message updating in VNs, and the LLR computation. For the first two steps, the messages are updated iteratively between the FNs and the VNs on the factor graph. Denote the maximum number of MPA iterations by J. Then the messages will be updated iteratively until $j = J$ is reached and the LLR will be computed by using the results of the iterative process. Wherein, the results from quantum search are used to update messages in the FNs, whereas both of the message updating step in the VNs and the LLR computation step are carried out in the classical processing phase.

In the step of message updating in FNs, a pair of equivalent CFs, i.e., $f^c_{n,k}(x_{[n]})$ and $f^q_{n,k}(a_{[n]})$ are defined in the classical processing phase and the quantum processing phase, respectively. Wherein, $x_{[n]} = \{x_{l,n}: l \in \emptyset(n)\}$ is a codeword combination at the n-th sub-carrier, $a_{[n]} = \{a_l: l \in \emptyset(n)\}$ is a M-dimensional vector denoted by $a_l = (a_{l,1}, a_{l,2}, \ldots, a_{l,M})$, $a_{l,m} \in \{0,1\}$ and $\sum_{m=1}^{M} a_{l,m} = 1$.

The message updating in FNs contains the quantum processing phase and the classical processing phase. In the quantum processing phase the entry $x^{max}_{[n]}$ that maximizes $f^c_{n,k}$ is found by a modified DH-QSA. (1) Specifically, the DH-QSA initializes a threshold δ randomly. (2) The specific input $a^s_{[n]}$ that satisfies $f^q_{n,k}(a^s_{[n]}) > \delta$ is termed as a solution. The DH-QSA interatively employs the Boyer-Brassard-Hoyer-Tapp Quantum Search Algorithm (BBHT-QSA) [16] for finding the solutions. (3) When a result is found by the BBHT-QSA, a codeword combination $x^s_{[n]}$ is determined by converting $a^s_{[n]}$ via a Q/C conversion. (4) The CF value $f^c_{n,k}(x^s_{[n]})$ is computed in the classical domain to check if it is a solution. Since $f^q_{n,k}$ and $f^c_{n,k}$ are equivalent, the CF value

$f^{q}_{n,k}(a^{s}_{[n]})$ is equivalent to $f^{c}_{n,k}(x^{s}_{[n]})$. (5) if $a^{s}_{[n]}$ is a solution, the threshold δ is updated to be $f^{c}_{n,k}(x^{s}_{[n]})$. The DH-QSA will terminate when no solution can be found or the maximized number of applying Grover operators has been exhausted. Finally, the $x^{max}_{[n]}$ will be found by the DH-QSA. In the classical processing, the FN updates the message $l^{j}_{n\rightarrow k}(x_k)$ in the classical domain as $f^{c}_{n,k}(x^{max}_{[n]})$. Then, the message obtained are forwarded to the neighbor VNs, as shown in Figure 3.4.

The message updated in the VNs as: $l^{j}_{n\leftarrow k}(x_k)=\sum_{u\in\psi(k)\backslash n} l^{j}_{u\rightarrow k}(x_k)$. Then the messages obtained are forwarded to the neighbor FNs. The above message updating steps between the FNs and VNs will be continuous until the maximum number of iterations is reached. Finally, the LLRs are computed when $j=J$ is reached. Specifically, the SCMA detector calculates the LLR of $c_{k,r}$ as $\lambda_1(c_{k,r})=\max_{x_k\in\chi^1(c_{k,r})} L(x_k)-\max_{x_k\in\chi^0(c_{k,r})} L(x_k)-\lambda^{P}_{2}(c_{k,r})$, where $L(x_k)=\sum_{n\in\psi(k)} l^{J}_{n\rightarrow k}(x_k)$.

Since the Q-MPA consists of the quantum processing phase and the classical processing phase, the total complexity of the Q-MPA is constituted by the sum of the complexity in the quantum domain and in the classical domain. Specifically, the complexity in the quantum domain is determined by the number of Grover operator applications, while the complexity in the classical domain is determined by the number of classical CF evaluations (CFEs) in calculation of CF $f^{c}_{n,k}(x_{[n]})$. We uses the idealized simplifying assumption that one Grover operator application in the quantum domain is equivalent to one CFE in the classical domain [17]. Table 3.1 shows a complexity comparison of lower bound between Classical MPA and Q-MPA. Where M represents codebook size and d_f represents degree of FN. In the Q-MPA, for each DHA the serach space is M^{d_f-1}. DHA can achive a complexity of search as $O(\sqrt{M^{d_f-1}})$. Since there are M SCMA codewords for each message updating in the FNs, the complexity of the Q-MPA is given by $O(\sqrt{M^{d_f+1}})$.

Table 3.1 Lower Bound of Complexity

Receiver	Complexity
Classical MPA	$O(M^{d_f})$
Q-MPA	$O(\sqrt{M^{d_f+1}})$

3.1.3 Performance Evaluation

Figure 3.5 illustrates numerical comparison of complexity between Classical MPA and Q-MPA. We characterize the complexity of the Q-MPA by the total Number of CFEs (NCFE), denoted by Ω_{QMPA}. The NCFE ratio is defined as $R_1 = \widetilde{\Omega}_{QMPA}/M^{d_f}$, where M^{d_f} is the NCFE of the classical MPA. From the figure we observe:

- The Q-MPA exhibits 45.55% of the classical MPA NCFE for M=16 and d_f=3.
- The average NCFE is only 11.57% higher than the theoretical NCFE lower-bound.
- The NCFE ratio curves decrease significantly as either M or d_f becomes higher.
- The lower NCFE imposed by the Q-MPA is because of applying fewer Grover operators in the quantum domain.

Therefore, this comparison demonstrates that the Q-MPA significantly reduces the NCFE of the classical MPA, especially when M and d_f are large.

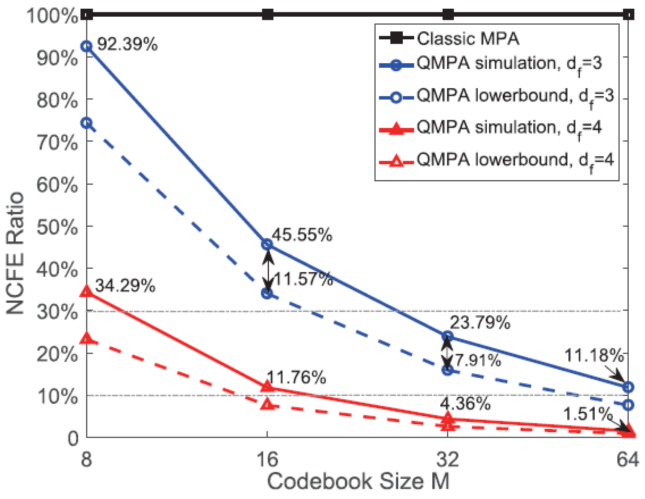


Figure 3.5 NCFE comparison between the classical MPA and the Q-MPA.

Figure 3.6 illustrates BER comparison between Classical MPA and Q-MPA. The basic parameters are set as follows: the number of users is K=6, the number of OFDM subcarriers is N=4, the degrees of the factor graph are d_f =3 and d_v=2. We adopt the SCMA codeword structure shown in Figure 3.2. Additionally, we employ a turbo code having an interleaver length of 1024 bits and coding rate of 1/3 as our channel code. From the figure we observe:

- The simulation curves of the Q-MPA overlap with MPA curves when the SNR is lower than 14 dB.
- The Q-MPA suffers less than 0.01 dB SNR penalty at 14.5 dB.

Thus, it shows that Q-MPA suffers only negligible BER performance degradation since the success probability of DH-QSA is slightly less than 1.

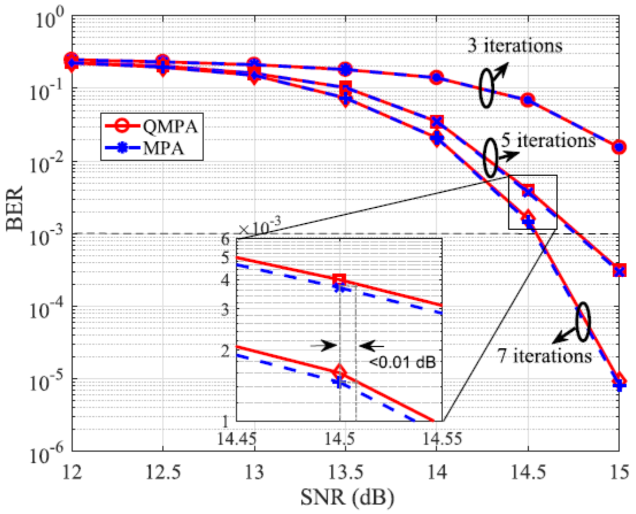


Figure 3.6 BER comparison between the classical MPA and the Q-MPA

3.2 Quantum Polar Code

Polar codes are capable of approaching Shannon’s capacity at a low encoding and decoding complexity, while conveniently supporting rate adaptation. Owing to these features, polar codes have found their way into the 5G and its subsequent versions. However, the data dependencies in the decoding process introduces high decoding latency. Inspired by quantum processing systems characterized by inherently parallel due to the quantum superposition, it is studied in [18] how to exploit this feature in dealing with decoding latency suffered by polar decoder by identifying isomorphism between the classical and quantum paradigms.

3.2.1 Polar code in the Classical Domain

Figure 3.7 shows an example of the encoding process as well as the successive cancellation (SC) decoding process for the polar code in the classical domain. The polar encoder is constructed by recusively invoking encoding kernel equipped with eXclusive OR (XOR) gate (labeld as G2 in Figure 3.7). As illustrated, an SC decoder operates on the same circuit as that of the encoder. However, while an encoder always processes the bits from left to right, an SC decoder operates from right to left as well as from left to right where the SC decoding is processed according to the sequence labeled by the numbers in parenthesis. Consequently, in the SC decoder, the information bits are serially recovered from top to bottom and thus introduce high decoding latency.

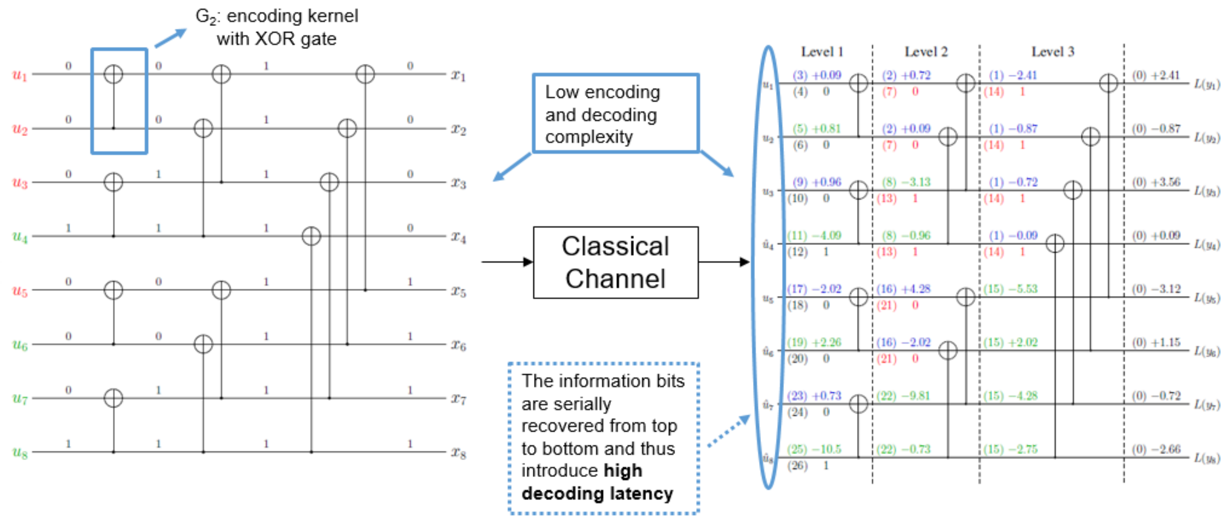
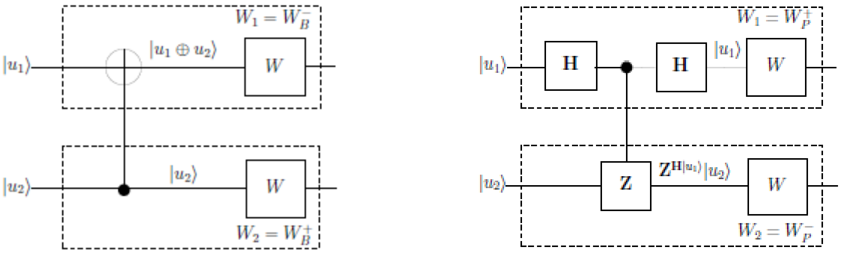


Figure 3.7 Example of the polar encoding process and SC decoding process

3.2.2 Polar code in the Quantum Domain

The classical depolarizing channel differ from its quantum counterpart in that the former only introduces bit-flip errors, while the latter imposes both bit-flip and phase-flip errors. The bridge between the classical and quantum paradigms relies on that a quantum depolarizing channel may be modeled by replacing XOR gates in classical polar codes with the quantum Controlled NOT (CNOT) gates to construct concurrently polarizing both the bit-flip and the phase-flip channels [19], as shown in Figure 3.8.



(a) polarized bit-flip channels (b) polarized phase-flip channels

Figure 3.8 The 2-qubit kernel of a quantum polar code in the Computational and Hadamard bases

An exemplary syndrome decoding based quantum polar code system is given by Figure 3.9. At the transmitter, a polar code polarizes the input quantum channels into the following four sets for a given [N, k, c] polar code:

- $\mathcal{F}^c$: Good bit-and-phase channels, for transmitting the uncoded k-qubits quantum information $|\psi\rangle$
- $\mathcal{F}_P$: Good bit-only channels, for transmitting Hadamard basis states $|z\rangle$ known to receiver
- $\mathcal{F}_B$: Good phase-only channels, for transmitting Computational basis sates $|x\rangle$ known to receiver
- $\mathcal{F}_{BP}$: Bad bit-and-phase channels, for transmitting c-ebits (whose one qubit is pre-shared to receiver)

Where, the (N-k-c) frozen qubits are transmitted by $\mathcal{F}_P$ and $\mathcal{F}_B$ channels. Then, the encoded qubits $\overline{|\psi\rangle}$ will be transmitted via quantum channel.

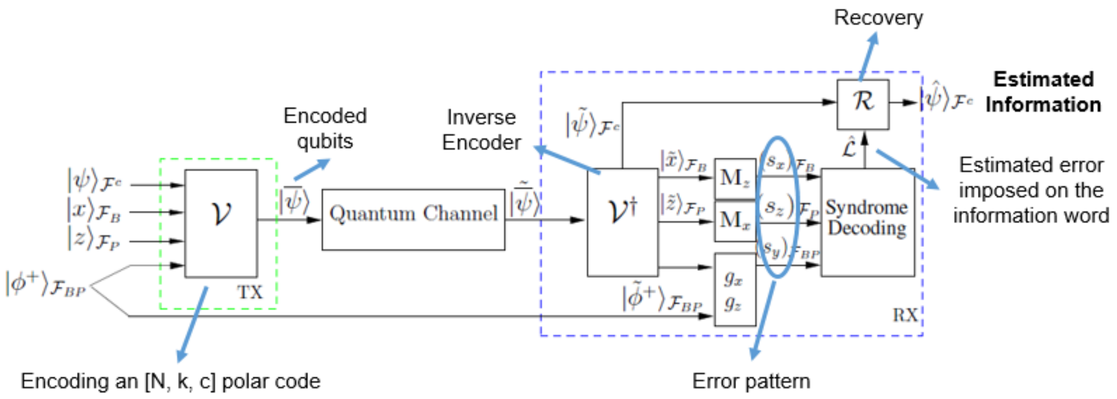


Figure 3.9 An exemplary syndrome decoding based quantum polar code system

At the receiver, the received information is passed through the inverse encoder $\mathcal{V}^\dagger$ to yield $|\tilde{\psi}\rangle$. The rest frozen quibits are passed through the inverse encoder to yield the error patterns s_x, s_z and s_y imposed on the frozen qubits, which are further fed to a syndrome-based polar decoder to obtain estimated error imposed on the information word. Finally, a recovery operation $\mathcal{R}$ is applied to $|\tilde{\psi}\rangle$ and the estimated error pattern $\hat{\mathcal{L}}$ to revover the transmitted information as $|\hat{\psi}\rangle$.

4 Reference

[1] https://ec.europa.eu/digital-single-market/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network?from=singlemessage&isappinstalled=0

[2] Publications Office of the European Union.JRC118150: Quantum Key Distribution In-field Implementations [R/OL].[2020-07-08]. http://publications.jrc.ec.europa.eu/repository/handle/JRC118150

[3] Quantum Flagship. Strategic Research Agenda of the Quantum Flagship[R]. Helsinki:European Quantum Flagship Event, 2020.

[4] Khan, I., et al., "Satellite-Based QKD." *Optics and Photonics News* 29(2): 26-33, 2018.

[5] Kimble, H. J., "The quantum internet." *Nature*, 453(7198): 1023, 2008

[6] U.S. Department of Energy. From Long-distance Entanglement to Building a Nationwide Quantum Internet: Report of the DOE Quantum Internet Blueprint Workshop[R/OL].[2020-07-08]. https://www.osti.gov/servlets/purl/1638794

[7] The Government Office for Science, UK, “The Quantum Age: technological opportunities”, 2016.

[8] Van Meter, R. and B.-S. Choi, "Applications of an entangled quantum Internet." network 15: 3, 2008.

[9] R. Wang et al., "End-to-End Quantum Secured Inter-Domain 5G Service Orchestration Over Dynamically Switched Flex-Grid Optical Networks Enabled by a q-ROADM," *Journal of Lightwave Technology*, vol. 38, no. 1, pp. 139-149, 1 Jan. 2020.

[10] https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20200113/Documents/Xavier_Priem.pdf

[11] https://www.bristol.ac.uk/physics/research/quantum/conferences/qkdover5guk/

[12] Valencia A., Scarcelli G., Shih Y H. “Distant clock synchronization using entangled photon pairs” *Appl. Phys. Lett.*, 85(13):2655-2657, 2004.

[13] Wehner, S., Elkouss, D. & Hanson, R. Quantum internet: a vision for the road ahead. Science 362, eaam9288 (2018).

[14] Wenjing Ye, Wei Chen, Xin Guo, Chen Sun, and Lajos Hanzo, "Quantum Search-Aided Multi-User Detection for Sparse Code Multiple Access, " *IEEE Access*, Apr. 2019.

[15] C. Durr and P. Hoyer, "A quantum algorithm for finding theminimum," Jan. 1999

[16] M. Boyer, G. Brassard, P. Høyer, and A. Tapp, "Tight bounds on quantum searching," *Fortschritte Phys., Progr. Phys.*, vol. 46, nos. 4-5, pp. 493-505, Apr. 1998.

[17] L. K. Grover, "A fast quantum mechanical algorithm for database search," *Proc. 28th Annu. ACM Symp. Theory Comput.*, pp. 212-219, May 1996.

[18] Z.Babar, A.Egilmez, LP.Xiang, D.Chandra, R.Maunder, S.X.Ng, and L.Hanzo, "Polar Codes and Their Quantum-Domain Counterparts, " *Communication Surveys & Tutorials*, 2019.

[19] M. Wilde and S. Guha, “Polar codes for degradable quantum channels,” *IEEE Transactions on Information Theory*, vol. 59, no. 7, pp. 4718-4729, Jul. 2013.

Acknowledgement

Grateful thanks to the following contributors for their wonderful work on this whitepaper:

Editors: Chih-Lin I (China Mobile), Xin GUO (Lenovo), Zhangchao MA (USTB)

Contributors:

Lenovo	Xin GUO
University of Science and Technology Beijing	Zhangchao MA, Jianquan WANG, Lei SUN
QuantumCTek, Co., Ltd.	Yong ZHAO
CAS Quantum Network, Co., Ltd.	Hao QIN

Abbreviation

AG	Advisory Group
AWGN	Additive White Gaussian Noise
BBHT	Boyer-Brassard-Hoyer-Tapp Algorithm
BER	Bit Error Rate
BS	Base Station
CF	Cost-Function
CFE	CF Evaluation
CNOT	Controlled NOT
DH-QSA	Durr-Hoyer Quantum Search Algorithm
DOE	Department of Energy
FG-QIT4N	Focus Group on Quantum Information Technology for Networks
FN	Function Nodes
ICT	Information and Communication Technology
ISG	Industry Specification Group

LLR	Log Likelihood Ratio
MPA	Message Passing Algorithm
MUD	Multi-User Detection
NCFE	Number of CFEs
NOMA	Non-Orthogonal Multiple Access
OFDM	Orthogonal Frequency Division Multiplexing
Q-MPA	Quantum-assisted MPA
QIN	Quantum Information Network
QIRG	Quantum Internet Research Group
QIT	Quantum Information Technology
QKD	Quantum Key Distribution
QMUD	Quantum MUD
QRNG	Quantum Random Number Generation
SC	Successive Cancellation
SCMA	Sparse Code Multiple Access
SDO	Standard Developing Organization
VN	Variable Nodes
XOR	eXclusive OR

FuTURE FORUM is committed to cutting edge technologies study and applications. Controversies on some technical road-maps and methodologies may arise from time to time. FuTURE FORUM encourages open discussion and exchange of ideas at all levels. The White Paper released by FuTURE FORUM represents the opinions which were agreed upon by all participating organizations and were supported by the majority of FuTURE FORUM members. The opinions contained in the White Paper does not necessarily represent a unanimous agreement of all FuTURE FORUM members.

FuTURE FORUM welcomes all experts and scholars' active participation in follow-on working group meetings and workshops. we also highly appreciate your valuable contribution to the FuTURE White Paper series.

未来移动通信论坛
FuTURE MOBILE COMMUNICATION FORUM