ZEISS SYMPOSIUM 2018
OPTICS IN THE
QUANTUM WORLD

WHITE PAPER ON QUANTUM COMPUTING AND QUANTUM COMMUNICATION

Based on the discussion during the respective workshop at the ZEISS Symposium "Optics in the Quantum World" on 18 April 2018 in Oberkochen, Germany

Executive summary

Quantum computing (QC) and quantum communication (QCom) are very promising in terms of commercial applications. Presently, however, both technologies face several roadblocks that need to be tackled in order to enable widespread commercialization. In both cases a stronger collaboration and exchange between industry and academia is required. Technology specific road blocks are:
For QC,

1. Limited open access to QC hardware.
2. Lack of good software, i.e., more QC algorithms that solve real-world problems.
3. A limited access to industrial manufacturing facilities makes it challenging to probe the scaling up of QC.
4. Technological challenges like limited qubit connectivity, too low gate fidelities, or large amounts of qubits required for error correction.
5. Missing business infrastructure, e.g., availability of long-term venture capital.
6. Brain drain (i.e. loss of knowledge, human resources, and IP) and a lack of knowledge protection.

For QCom,

1. Challenge of performing quantum cryptography within existing fiber infrastructure as well as the software, i.e., combining quantum cryptography algorithms and classical cryptography.
2. The benefits of quantum cryptography and its area of application (long term security) have to be communicated clearly by the QCom community.

To tackle these challenges the following actions are proposed:

1. Greater access to both industrial and government facilities (manufacturing infrastructure).
2. Actions should be taken to facilitate the collaboration between industry and academia (e.g. quantum hubs in the UK).
3. Guided by improved coordination between natural sciences and engineering faculties, university curricula should become more interdisciplinary to enable better collaboration between industry and academia.
4. Policies for the protection of knowledge are needed to combat the brain drain in Europe.
5. Interdisciplinary research initiatives are required to develop and establish quantum cryptography as a cryptographic primitive in the toolbox of modern cyber security.
6. Quantum engineering is needed to facilitate the transfer from science to commercial applications.

Preface and introduction

Today, quantum technologies (QT) form the basic technology for many branches of industry. These include the groundbreaking technologies of transistors in the semiconductor industry, lasers and light-emitting-diodes in telecommunication, image detectors in computer vision, and atomic clocks in global positioning systems.

A second wave of quantum technologies, based on the ability to control the quantum state of a single or a few coupled quantum systems, such as single atoms, single ions, and single photons is about to transition from academic research to commercial applications.

Among others, this second wave provides new paradigms and methods for processing and transmitting information.

Quantum computing (QC) provides a new paradigm for computing with the potential to solve certain computational problems much faster than by using classical computing architectures.

Quantum communication (QCom) provides new cryptographic primitives for fundamentally secure communication such as secure key exchange between remote parties and the generation of true random numbers.

This white paper provides a summary of the discussion between representatives of industry and academia, which took place during the workshop on quantum computing and quantum communication at the ZEISS Symposium "Optics in the Quantum World" on 18 April 2018 in Oberkochen, Germany.

This white paper is divided into four parts:

1. Opportunities provided by QC & QCom
2. Current status of QC & QCom
3. Current challenges and potential obstacles on the road towards commercialization
4. Actions required to enable the commercialization of the technologies

Opportunities provided by QC & QCom

The term **quantum computing** encompasses at least three technology stages: quantum annealing (QA), non-error-corrected QC and fully error-corrected QC. Going from one stage to the next increases the technical complexity but also offers more potential benefits and opens QC up to additional applications. QA promises a solution to hard optimization problems with potential applications for artificial intelligence and logistics. Non-error-corrected QC enables the simulation of quantum systems with potential applications in chemistry, medicine and material science. Finally, fully error-corrected QC promises exponential speed-ups for specific algorithms. Potential applications include cryptography and database searches.

Quantum communication provides methods for enabling secure communication. To that end, quantum random number generators can be used to provide true random numbers. Quantum key distribution (QKD) provides verifiably secure communication between remote parties that does not rely on assumptions of computational complexity as opposed to classical cryptography. Quantum key distribution over distances can form a bridge, depending on the hardware used. Fiber-based QKD allows distances of up to 300 km. Satellite-based QKD extends the range to thousands of kilometers, though the available key rates differ greatly depending on the hardware and distance chosen. Similar to classical repeaters, quantum repeaters can be used to combat noise in the signal and further enhance the range achievable with a given hardware platform. More range enables networks of increasing complexity. While in a trusted node network, a sender (A) still has to rely on a trusted intermediate node (B) to pass on a signal to a distant receiver (C) due to limited range, in a fully quantum network he can send a message to C without having to trust any intermediate parties.

Current status of QC & QCom

For both quantum computing and quantum communication, the participants of the quantum computation and quantum communication workshop estimated that the potential of the technologies for commercial applications (based on the opportunities listed in the previous section) is in the range between medium and high. The participants of the workshop took part in a survey to estimate the time to first commercial products and the position of the technologies on the Gartner hype cycle. The results of this survey are shown in Figure 1. For QC, only QA devices are already commercially available. According to our survey, QA has already passed the "Peak of Inflated Expectations", whereas both non-error-corrected and fully error-corrected QC are still within the "Technology Trigger" phase. For non-error-corrected QC, the first commercial products are expected to be available in 6 years and for fully error-corrected QC in more than 15 years.

The QCom results indicate a more mature stage of the technology. Both quantum random number generators and fiber-based QKD are already commercially available and, according to our survey, are already within the "Through of Disillusionment". The first commercial products for trusted node networks are expected to be available 4 years from now. Commercialization of the satellite-based QKD will take more than 7 years. While satellite-based QKD is on its way to the "Peak of Inflated Expectations", trusted node networks have already passed it. The first products for quantum repeaters are predicted to be more than 8 years away, only surpassed by fully quantum networks for which we will have to wait 10 more years. In line with that assessment, both technologies are still at the innovation trigger point.

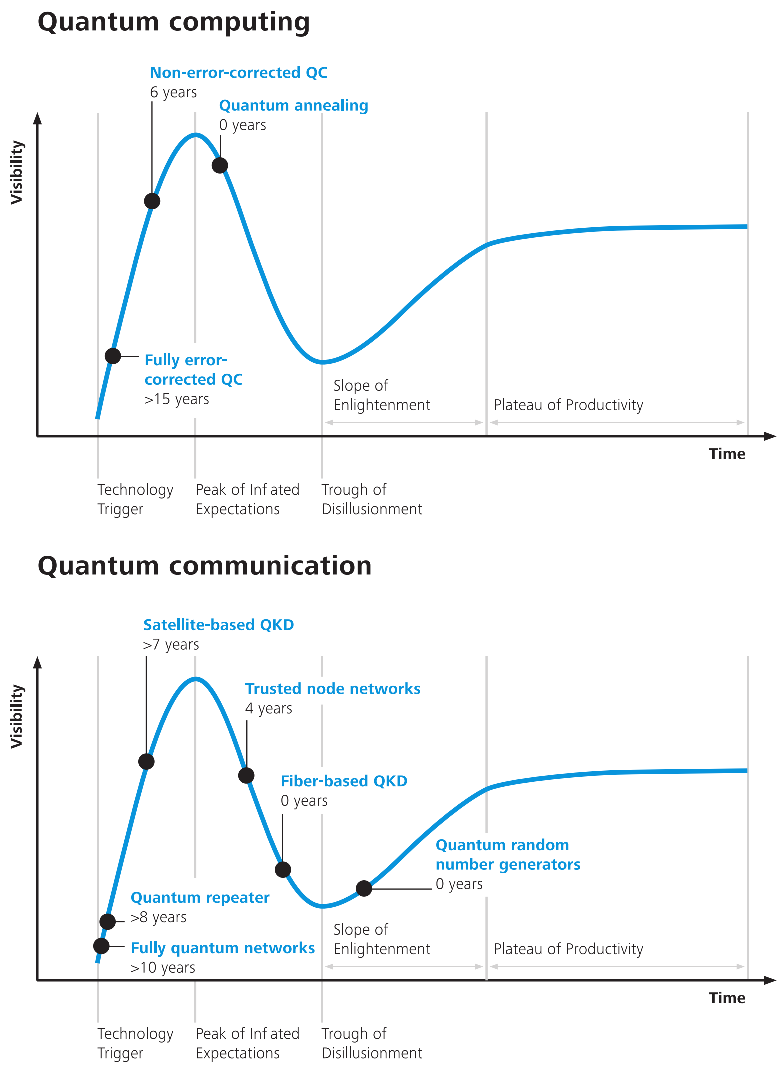

Figure 1: Hype cycles for quantum computing and quantum communication. The times below the technologies indicate the expected time to the first commercial product (first commercial niche applications) for the different technologies. The estimates depicted above are based on a survey conducted among the participants of the quantum computing and quantum communication workshop.

Current challenges and potential obstacles on the road towards commercialization

QC and QCom are very promising in terms of commercial applications. Presently, however, both technologies face several roadblocks that need to be tackled in order to enable widespread commercialization. Some of those roadblocks are common to both technologies while others are specific to either QC or QCom. In general, a lack of interdisciplinary education in physics and engineering makes it difficult to bridge the gap between basic research and real-world products for both technologies. For both technologies a stronger collaboration and exchange between industry and academia is required.

For QC, limited access to QC hardware and a deeper understanding of how to leverage the potential of QC (more fundamental research is required) hinder the development of quantum software. This lack of good software, i.e. more QC algorithms that solve real-world problems, is still preventing a strong marked pull. Limited access to industrial manufacturing facilities makes it difficult to probe the scaling-up of QC. Finally, we face technological challenges like limited qubit connectivity, too-low gate fidelities, and large amounts of qubits required for error correction. Some challenges are specific to the QC ecosystem in Europe: these include missing business infrastructure, e.g. the availability of long-term venture capital, the brain drain (i.e. loss of knowledge, human resources, and IP), and a lack of knowledge protection.

For QCom, widespread adoption is hindered by a communication and education gap. The benefits of quantum cryptography and its area of application (long-term security) have to be communicated clearly by the QCom community. Furthermore, the fact that it remains difficult to combine architectures for quantum cryptography with existing classical communication setups creates a barrier that prevents potential users from adopting this technology. This concerns both the hardware, i.e. the difficulty of performing quantum cryptography within an existing fiber infrastructure, and the software, i.e. the challenge of combining quantum cryptography algorithms and classical cryptography. A lack of interdisciplinary education makes it difficult to bridge the gap between classical and quantum communication experts. In general, there seems to be too little public awareness regarding the benefits and the scope of quantum cryptography. Finally, there are technological challenges like the lack of quantum memories and infrastructure issues like missing acknowledged standards and certification authorities.

Actions required to enable the commercialization of the technologies

The participants of the workshop developed several action items during an open discussion.
In view of its infrastructure issues, quantum computing would benefit from increased access to both industrial and government facilities (manufacturing infrastructure). Furthermore, having the government as an early adopter of quantum hardware would make it easier for startups to bridge long timespans between the initial prototype and the final product. Policies for the protection of knowledge are needed to combat the brain drain in Europe in order to capitalize on the investments in fundamental research as soon as quantum technologies become commercially viable. Solving the technological issues requires continued funding of fundamental research. Guided by improved coordination between natural sciences and engineering faculties, university curricula should become more interdisciplinary.
For QCom, interdisciplinary research initiatives are required to develop and to establish quantum cryptography as the cryptographic primitive in the toolbox of modern cyber security. Continued support of the enabling-technologies ecosystem and fundamental research funding is needed to find a solution to the technological challenges.
Finally, for both QC and QCom, actions should be taken to facilitate the collaboration between industry and academia (e.g. quantum hubs in the UK). A strong collaboration between industry and academia is needed in order to demonstrate the benefits of QC and QCom for practical application and to drive the adoption of the technologies – the Symposium "Optics in the Quantum World" was one step and a small contribution towards bringing both parties together.