2. Future quantum technologies

*By Matthias **Troyer** (Distinguished Scientist, Microsoft Quantum), with contributions from Rob **Thew** (Senior Researcher Quantum Technologies, University of Geneva), Francesco **Petruccione** (Pro Vice-Chancellor Big Data and Informatics, University KwaZulu-Natal), Peter **Knight** (Imperial College London), Nicolas **Gisin** (Professor for Quantum Information and Communication, University of Geneva) and Philipp **Treutlein** (Professor at University of Basel) and edited by Daniel **Saraga**.*

Key Concepts

Quantum physics describes the behavior of particles at microscopic scale. **Quantum technologies** harness the specificities of quantum properties to improve on standard technologies. They make use of **superposition** of multiple classical states and **entanglement**, which is a non-local property shared by particles which are separated but whose behaviors are intertwined. These allow cryptographic keys to be shared securely over hundreds of kilometers, quantum computers to solve classically intractable problems and quantum sensors to reach unprecedented precision. As future quantum computers will be able to crack most of the current encryption techniques (in particular, RSA), new encryptions schemes must be developed and deployed already today in order to secure documents also in the future. This is the goal of **quantum-resistant cryptography.**

Scientific Anticipatory Brief abstract

Current status of research

Quantum technologies harness specific quantum properties of matter at microscopic scales to improve on standard technologies. They traditionally encompass three types of technologies. **Quantum communication** systems are already commercialized today and offer dedicated secure communication channels over up to a few hundred kilometers as well as the generation of truly random numbers, e.g. in finance. **Quantum computers** have demonstrated superiority over classical computers for testing purposes but not yet for applications. An increasing number of **quantum sensors** that leverage non-trivial quantum effects are being developed and commercialized (e.g. for medical imaging, or for geological surveys), including magnetic detectors, gravitational sensors and ultraprecise clocks (needed e.g. for GPS satellites).

Trends at 10 years - quantum advantage for academic problems and quantum communication networks

In the next decade quantum communication channels will expand to build networks with several nodes connecting locations more than 500km apart. Quantum computers will increasingly demonstrate advantages over classical machines in varied academic problems. Quantum sensors will be deployed for various applications: gravitational sensors are used for geological surveys, accelerometers and gyroscopes help autonomous transport, new magnetic detectors make portable MRI medical imaging possible, temperature and pressure sensors improve weather forecast, and gas spectrometers improve climate change modelling. Sensing devices will be connected via quantum communication links to share entanglement and increase their precision even further.

Trends at 25 years - quantum internet, universal quantum computers and new insights in quantum biology

On the 25-year horizon, a “quantum internet” will enable a new level of data privacy for both communication and computation. Universal quantum computers will run any quantum algorithm. **Their ability to crack the current RSA encryption algorithm will raise the issue of data security and the need to control access to quantum computation systems.** Quantum computers will very accurately simulate chemical compounds, leading to computational discoveries in areas such as chemical catalysis (important for carbon fixation for climate change mitigation and nitrogen fixation for fertilizers) and new materials (such as smart functional materials with switchable properties and, possibly, higher temperature superconductors). Quantum computers will run quantum machine learning algorithms for problems with small data sets and for applications yet to be discovered. Quantum sensors will be deployed in many industrial and research settings.

In the area of quantum biology, the analysis of quantum effects in biology – especially in the brain – is a rapidly evolving field. Little is currently known about whether quantum effects are really involved in biological processes, but an increasing amount of research will study and measure them in the next decade, before aiming to influence them for better health outcomes on the 25-year horizon.

Potential consequences on people, society and the planet

Quantum technologies will have **global impacts.** They will call for the **training of a quantum-aware workforce with expert skills, which will be the subject of global competition for talent.** As quantum communication and computing can respectively increase data privacy and break current encryption methods, they are both highly **relevant to national security and exporting them will be subject to increasing control.** By driving discoveries in chemistry and material science, quantum computers will **help address the planet’s biggest challenges, in particular energy management, climate change mitigation and food production,** while quantum sensors will improve diagnostic precision and disease monitoring. Discoveries in the field of quantum biology could bring a new understanding of basic biological processes and quantum effects in the brain, which could potentially lead to new therapies in the long term.

Detailed table overview of trends at 5, 10 and 25 years

2. Future quantum technologies

Example of breakthroughs

5 years	10 years	25 years
Quantum computing		
• Noisy Intermediate Scale quantum (NISQ) computing (50-100 qbits) • Special purpose quantum devices helping researchers (sensors, simulators, ...)	• **Quantum advantage for real problems**, the first fault tolerant scalable computer • Simulators of quantum dynamics • Quantum-driven discoveries and modelling (effective models for quantum effects in materials...)	• Large scale quantum computing - Universal quantum computers with a million qubits include error-correction techniques and can run any quantum software • Any encryption systems based on the current RSA technique can be cracked by Shor's algorithm • Catalysis (carbon, nitrogen fixation, clean energy, water) and chemical reaction mechanisms • Emergence of new quantum applications and quantum-inspired approaches, e.g.in machine learning • Access control on quantum computation desired instead of export control
Quantum communication		
• Information networks using quantum key distribution with trusted repeaters • **Quantum resistant cryptography**	• Terrestrial and satellite links quantum cryptographic secure channels over more than 500 km. • Device-independent protocols enable the certification of encryption systems. • **Unconditionally secure communication**	• **Large-scale quantum network for secure quantum computations** (pan European Quantum Internet, US, China,..) • **Unconditionally secure computation**
Quantum sensing		
• Quantum sensors for biological sensing and medical purposes (Quantum MRI Quantum effects in the brain as research field of study • Quantum gravity detectors are deployed for geological survey and earthquake monitoring	• Improved quantum sensors for medical diagnostics • Influencing the body and the brain through quantum effects	• **Quantum effects in biology and neurosciences evolving into applications**