

Quantum information technology

Kae NEMOTO¹, Masahide SASAKI², and Gerard MILBURN³

¹*National Institute of Informatics*

²*National Institute of Information and Communications Technology*

³*School of Mathematics and Physics, The University of Queensland*

The basic ideas in quantum information processing (QIP) dates from several decades back, however the research development based on these ideas started only a little more than a decade ago. The initial ideas of quantum information processing emerged from the fundamental difference between quantum physics and classical physics. It was, and still is, hard to analyse quantum systems in general, and in particular when a quantum system gets bigger, it soon becomes intractable even with high performance computers. To analyse a quantum system, Feynman suggested that we should use a computer based on quantum physics. This is the initial idea of quantum information processing. By contrast to quantum computers, all non-quantum-physics-based computers, that is, all the existing ones including high performance computers, are now called “classical computers” indicating computers based on classical physics.

The research on quantum information processing did not take off until 1990s. Until then, the technology to manipulate quantum was yet not ready, and more importantly, the theory for QIP was not developed enough to show the way to efficiently use quantum nature to carry out computation. Quantum key distribution (QKD) was one of the first QIP protocols successfully implemented and developed in 1990s.

QKD is a protocol to exchange secure key material between authenticated users at a distance. Thanks to a property that overlapping quantum states cannot be cloned without trace of interaction, the protocol can detect an eavesdropper by measuring the quantum states and post-processing the signals via classical communication between the users. As one-time pad using QKD was proven to be secure against an eavesdropper who has unbounded ability, unlike conventional cryptogra-

phy relying on computational complexity, QKD initiated a huge research effort. It has driven significant improvement of non-classical light sources and novel photon detection.

Later, this became the technological basis for linear optics quantum computation which emerged at the very end of the last century. In the 1990s, there are some experimental milestones such as the observation of entanglement, i.e. quantum correlation and the first teleportation experiments, however more noticeably the last missing part in QIP was fulfilled by the discovery of quantum error correction and Shor’s quantum algorithm. These theoretical advances in 1990s together with the state-of-art technology in labs initiated a tremendous research effort worldwide.

Turning to this century, in the first decade, the rapid experimental developments together with nanomanufacture and -manipulation are most noticeable. In many different physical systems, more qubits are now implemented and fundamental protocols such as entangling gates and teleportation have been demonstrated and further improved to higher fidelity. In optics, QKD has been steadily improved in key rates and communication distance. The security proofs become available and the QKD research is now shifting from the fundamental research to commercial development. This special issue includes a paper on this topic showing some accepts of the current status of QKD. For more general and demanding QIP tasks involving multi-qubit operations, optics had a fundamental problem with the lack of photon-photon interaction.

In 2000, linear optics quantum computation (LOQC) took off with the theoretical discovery of the computational power of non-deterministic operations with passive linear optical elements and post-selection. LOQC has pushed the system to the size of several qubits, demonstrating the fundamental entangling gates such

Received January 18, 2011.

¹nemoto@nii.ac.jp, ²psasaki@nict.go.jp, ³milburn@physics.uq.edu.au

DOI: 10.2201/NiiPi.2011.8.0

as ControlledNOT gate. Then it was soon running the race of system size with other more matured systems such as ion-traps. With optical system, we can treat more qubits than other systems allow us to do, while ion-trap implementations show advantage of the high fidelity gate, state manipulation. Other physical systems, such as superconducting qubits and quantum dots, have traced a similar path.

Although many different physical systems have demonstrated the proof of principles of QIP, each system has its own advantages and disadvantages to scale up the QIP system. Quantum nature is fragile to errors and losses, and hence it is a daunting task to achieve the necessary interaction without decoherence. The experimental efforts revealed novel properties of quantum nature and our understanding in quantum physics deepened, however these quantum systems and manipulations are not particularly suitable as building blocks and devices to build quantum information systems. Each physical system exhibits different difficulties to scale the system up, and yet theoretical research on error correction and fault-tolerance indicates the high overhead for quantum error correction requiring millions of qubits for middle to large scale quantum information processing. One qubit by qubit scaling in the current implementation cannot be extended to such a scale. From the viewpoint of quantum information technology, this research path seems to require a fundamental breakthrough.

To bridge the gap in scales, theoretical research took a different direction to show the requirements for fundamental building blocks for larger scale quantum systems. It suggests a shift to hybrid systems integrating different physical resources. The merit of this direction is clearly to exploit the advantages from each physical component bypassing their disadvantages, however at the same time the design of fundamental QIP building blocks becomes more challenging to implement.

From the view of scalability, the most significant aspect of hybrid systems is to give the device design more flexibility and hence the QIP system becomes more flexible to adapt system architecture.

In 2009, finally the first scalable large-scale optical quantum computer architecture was laid out, showing a hybrid atom-photon module to be the fundamental building block. This is a good starting point to discuss the requirements for quantum devices to be able to assemble a quantum information system. The development of quantum devices which serve as building blocks for scalable architecture is increasingly important for the QIP as a future technology. Due to the hybrid nature, building blocks such as the hybrid atom-photon module may be significantly more difficult to implement than current device designs, however

nonetheless experimental efforts towards this direction have already seen. The special issue shows several new important implementations and ideas along this line.

To accelerate the development, clearly it is necessary to bring people and expertise together from different backgrounds. This recent trend certainly indicates the pathway for quantum information technology. It hence seems timely to discuss the possible foundations of future quantum information technology. This special issue focuses the new trends and developments in quantum information technology, showcasing the new developments in the field of quantum information and computation from theoretical aspects to engineering issues. Its particular emphases are on integrated chip-based devices, matter-light hybrid systems, system architecture for QIP, and engineering issues in quantum information systems. Within the framework, this issue broadly covers aspects from different material platforms, fabrication approaches, new designs and optimization concepts of devices, together with the theoretical investigation of related quantum phenomena. In October 2010, the second international conference on quantum information technology was held at NII to share the same research direction and purpose to this special issue, and the presentations at the conference were also invited to contribute to it.

The special issue has selected eleven papers including from QKD to high performance quantum computation. All of the papers exhibit an important aspect of quantum information technology to be further developed. We, the guest editors, would like to thank the authors contributed to the special issue and researchers who participated and contributed to the discussions in the conference. We also would like to express the deep appreciation to the referees who worked with us through the tight schedule. The research field requires intellectual interaction more than ever across science and engineering for this promising future technology to be realized. We hope that this special issue will be found also useful to initiate such interdisciplinary research efforts in the future.

**Kae NEMOTO**

Kae NEMOTO is a Professor in the Principles of Informatics Research Division at the National Institute of Informatics, Tokyo, Japan. She heads the Quantum Information Science Theory Group and is a leader in the Japanese-France Laboratory for Informatics. Her research interests and efforts are currently focused around the implementation of quantum devices, architectures for large-scale QIP, quantum/atom optics and quantum nonlinear dynamics.

**Masahide SASAKI**

Masahide SASAKI received the B.S., M.S., and Ph.D. degrees in physics from Tohoku University, Sendai Japan, in 1986, 1988 and 1992, respectively. During 1992-1996, he worked on the development of Si-MOSFET with Ayase Laboratory, Nippon Kokan Company, Kanagawa Japan. In 1996, he joined the Communications Research Laboratory, Ministry of Posts and Telecommunications (since 2004, National Institute of Information and Communications Technology, Ministry of Internal Affairs and Communications). Since 1994, he has been working on Quantum Information Theory and Quantum Optics. He is presently group leader of the Quantum ICT group. Dr. Sasaki is a member of Japanese Society of Physics, and the Institute of Electronics, Information and Communication Engineers of Japan.

**Gerard MILBURN**

Gerard MILBURN obtained a PhD in theoretical Physics from the University of Waikato in 1982 for work on squeezed states of light and quantum nondemolition measurements. He is currently an Australian Research Council Federation Fellow at the University of Queensland and Director of the new Australian Research Council Centre of Excellence in Engineered Quantum Systems. Gerard Milburn is a Fellow of the Australian Academy of Science and The American Physical Society. He has worked in the fields of quantum optics, quantum measurement and stochastic processes, atom optics, quantum chaos, mesoscopic electronics, quantum information and quantum computation, and most recently in quantum nanomechanics and superconducting circuit QED. He has published over 200 papers in international journals. He has published four books. Together with Dan Walls he published one of the first texts on Quantum Optics (Springer 1994), recently updated with a new edition (Springer, 2008), and two non technical books on quantum technology and quantum computing (Schroedinger's Machines, Allen and Unwin, 1996; The Feynman Processor, Allen and Unwin 1998) and Quantum Measurement and Control with Howard Wiseman, (Cambridge University Press, 2010).