Quantum Information Science: An Update

L.C. Kwek
Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543, Singapore.
Institute of Advanced Studies, Nanyang Technological University, 60 Nanyang View, Singapore 639673, Singapore.
National Institute of Education, Nanyang Technological University, 1 Nanyang Walk, Singapore 637616, Singapore.
MajuLab, CNRS-UNS-NUS-NTU International Joint Research Unit, UMI 3654, Singapore

Freddy P. Zen
Institut Teknologi Bandung, Bandung 40132, West Java, Indonesia.

Abstract. It is now roughly thirty years since the incipient ideas on quantum information science were concretely formalized. Over the last three decades, there has been much development in this field, and at least one technology, namely devices for quantum cryptography, is now commercialized. Yet, the holy grail of a workable quantum computing machine still lies faraway at the horizon. In any case, it took nearly several centuries before the vacuum tubes were invented after the first mechanical calculating were constructed, and several decades later, for the transistor to bring the current computer technology to fruition. In this review, we provide a short survey of the current development and progress in quantum information science. It clearly does not do justice to the amount of work in the past thirty years. Nevertheless, despite the modest attempt, this review hopes to induce younger researchers into this exciting field.

1. QUANTUM COMPUTER

Each time you send secure information over the internet, for instance, credit card numbers and so forth, we rely on the simple idea that although it is easy to multiply two large prime numbers, it is difficult to perform the reverse process of factorization. Locking information relies on the multiplication of two large prime numbers and so it is generally easy. However, to unlock the information, we need to do the reverse process of factorization, which is difficult. Secure communication systems based on the relatively hard prime number factorization process have been invented, the most popular algorithm being the RSA gate.

Although David Deutsch showed that one could design quantum circuits and algorithms with quantum logic, the idea that one could build a computer based on quantum mechanical principles flies only after Peter Shor showed in 1994 that if the relatively secure prime number factorization could be broken if we can build a quantum computer.

It is interesting to trace the history of computing machines: from the abacus to the slide rule and from the babbage machines to the first huge calculating machine, the ENIAC. An amazing fact that we learnt from history is that it takes a long time before a mechanical calculator was even built. But once the proper technology was discovered, in this case the invention of
the transistor, there was an exponential progress in the development of the calculator and the computer.

Our current (classical) computer works on binary logic: low and high voltages. Information are encoded with binary or base 2 numbers. All logical operates are performed with fast logic gates on these numbers. Like a classical computer, a quantum computer on the other hand can operate on binary states, say low and high energy states, but it possesses one extra ingredient that is absent from the classical systems. A quantum computer can operate on low and high energy state as well as any superposed states of low and high energy. In short, a quantum computer operates on the quantum state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where $\alpha$ and $\beta$ are both complex numbers. This state is also known as the quantum bit or qubit.

A superposed state is somewhat analogous to the situation in Fig 1 where one is shown an illusory picture of a young lady with her head turned from the audience and an old woman smiling. Depending on where one focuses on the picture, one sees either a young lady ($|0\rangle$) or an old woman ($|1\rangle$). However, just as in quantum theory, as soon as one focuses on the young lady, one loses the image of the old woman. Thus, any measurement on a superposed state of the two quantities ($|0\rangle$ or $|1\rangle$) collapses the wavefunction into one of the states.

![Figure 1. The typical illusory picture of a young lady with her head turned and an old woman smiling provides a good metaphor for a superposed state of a young lady or an old woman. Moreover, if one focus on the young lady, one tends to lose the picture of the old woman and vice versa, showing that measurement “destroys” superposition.](image)

Naively, it means that for a classical computer that evaluates a function $f$ on all three-bit numbers, it would essentially need to compute $f(000), f(001), f(010), \cdots f(111)$. In contrast, a quantum computer simply operates on the superposed state $\frac{1}{8}(|000\rangle + |010\rangle + \cdots |111\rangle)$ to yield $f \left( \frac{1}{8}(|000\rangle + |010\rangle + \cdots |111\rangle) \right)$. This is as if one operates on a “massively” parallel computer. But, of course, here we are naively simplifying the whole matter, in principle a quantum computer needs more than just linear superposition, see Fig. 2. Technically a three-qubit state, say $|010\rangle$ should be written as $|0\rangle \otimes |1\rangle \otimes |0\rangle$.

Everybody in the electronics industry now know that a major component of the computer is the NAND (not-AND) gate. With this component, all machine codes (realizing arbitrary algorithms) can be constructed. We call this component a universal gate, since even single-bit gate like the NOT gate can be build from a NAND gate by simply parsing the same input.
A quantum bit is a superposed state of both $|0\rangle$ and $|1\rangle$ and so there is “effectively” some form of parallel computing in the scheme.

into the two input ports of the NAND gate, and we say that the machine that are made from such components, a universal computing machine. It was shown a long time ago [1, 2] that a key theoretical ingredient for a universal computing if one uses a quantum computer is the realization of an arbitrary single-qubit gate and any two-qubit entangling gate. A single-qubit gate is straightforward. It consists of an input that takes in a quantum bit and performs an arbitrary unitary operation on the state. An entangling gate on the other hand has an input that takes in a superposed state of two quantum bits (it can be trivial, the input state could be just $|0\rangle \otimes |0\rangle$) and spits out a quantum state that cannot be written as a separable form $(\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha'|0\rangle + \beta'|1\rangle)$.

There has been much progress since the eighties on the development of this dream of a quantum computer. In particular, Chris Monroe et al showed in 1995 that an entangling gate can be built using ion-trap technology [3] and a fully scalable universal gates based on ion trap is also possible [4]. But apart from ion trap, feasibility of universal computation with few qubits have also been shown in several other platforms like nuclear magnetic resonance devices [5, 6], integrated photonics chips [7, 8, 9, 10], cavity QED [11, 12], circuit QED with flux and phase superconducting qubits [13, 14] and so forth. However, scalability is an important benchmark and it is not obvious which platform is ultimately going to be the winner in terms of large scale scalability.

2. QUANTUM SIMULATORS

Although nobody can say for sure when a fully functional quantum computer will be built, there is another promising direction with current ultra-cold atoms and quantum technologies. In a keynote speech at the MIT Physics of Computation Conference in 1981, and published subsequently in Ref. [15], Richard Feynman remarked that “nature isn’t classical, dammit, and if you want to make a simulation of nature, you’d better make it quantum mechanical”. In fact, he added that he would “like to have an exact simulation, in other words, that the computer will do ‘exactly’ the same as nature”. In recent years, the ability to tune and control one quantum system to simulate or emulate another physical quantum mechanical system has been provably
What does a quantum simulator do? Suppose we need to understand a physical system that is well described by some Hamiltonian $H_0$ with some initial state $\psi_0$. Suppose also we have a system of particles (atoms or molecules) in a constrained environment, for instance, trapped in a hollow fiber or a harmonic trap, that is approximated by some tunable Hamiltonian $H_1(\Delta_1, \Delta_2, \cdots)$ and controllable initial state $|\psi_1(\delta_1, \delta_2, \cdots)\rangle$ where $\Delta_1, \Delta_2, \cdots$ and $\delta_1, \delta_2, \cdots$ are some tunable or controllable parameters. If one could tune the Hamiltonian $H_1$ and $|\psi_1\rangle$ so that $H_1(\Delta^0_1, \Delta^0_2, \cdots) \approx H_0$ and $|\psi_1(\delta^0_1, \delta^0_2, \cdots)\rangle \approx |\psi_0\rangle$, then we see that the tunable system $H_1$ will in principle mimic the dynamics of $H_0$ and so $H_1$ acts as a quantum simulator for $H_0$ [16].

Quantum systems are well known to be notoriously difficult to analyze with increasing number of particles as the state of $N$ spin-1/2 particles requires a memory of $2^N$ complex numbers, even if one were to ignore the motional degrees of freedom. Time evolution of such a system requires even more computation, involving a $2^N \times 2^N$ matrix. On the other hand, for experimental realization of physical systems, it is generally easier to consider large $N$, though not all controllable. Thus, quantum simulation provides a valuable tool for researchers from numerous fields, ranging from condensed matter physics to material sciences to chemistry and even biology. There are countless of interesting yet unsolved puzzles in Science involving many-body problems. A good understanding of many-body systems, for instance, in high temperature superconductivity will push the frontier of our knowledge to the next level.

The recent flurry of activities in quantum simulators on various platforms, cold atoms trapped in ion traps, optical lattices and hollow fibers as well as photons in waveguides have shown the feasibility of performing simulations with quantum systems. The main idea is to trap ultra-cold atoms or molecules in an ion or optical traps. In particular, optical lattices can be realized with two or more interfering laser beams that form standing waves interacting with the atoms or molecules. The optical potential can be tuned in situ by varying its intensity, frequency and phases. To date, several proof-of-principle experiments have been successfully performed on this platform. In particular, it has been shown that cold atomic gases trapped in optical lattices exhibit transition from the superfluid to Mott-Insulator phases as well as show the crossover from a Bardeen-Cooper-Schrieffer (BCS) state of weakly attractive fermions to a BEC of tightly bound pairs [17, 18, 19, 20].

Bolder schemes based on loading dilute cold atom gases into a hollow fiber have also been proposed [21]. In one scheme, a strongly correlated quantum gase of polaritons is created using one-dimensional optical systems, namely hollow fiber, with tight field confinement. The Hamiltonian for the physical system is found to be mapped into a strongly correlated system of one-dimensional bose (or fermi) gas. With modifications to the configurations, one could also mimic Luttinger liquid (showing charge-spin separation) or the massive Thirring models [22, 23] (see Fig. 3).

3. QUANTUM COMMUNICATION

To date, no quantum computer can solve a problem that a classical computer cannot do so. However, there is a technology that quantum information science has somewhat bring to fruition. Devices for quantum cryptography, albeit expensive, are now readily available off the shelf. The market is not large nor interested, partly due to the exorbitant cost. However, the device is there, and depending on the paranoia over security, one could in principle engage somebody to build the World’s most secure system to date.

One of the main motivations for the construction of a quantum computer is that a quantum machine using superposed states and possibly entanglement can tremendously speed up the factorization of two large numbers. To give an idea, a typical 640-bit number that is composed
of two prime numbers needs roughly $30 \times 2.2$ GHz Opteron-CPU years, which translates to roughly over five calendar months. The reverse operation of multiply two large primes to give a larger primes is easier. Such number indeed underlies the working mechanism of a current encryption scheme, called the Rivest-Shamir-Alderman (RSA) scheme. The easy process of multiplying two large prime numbers is used for encoding secret or secure information, for instance the credit card number. To decode the information, one needs the reverse process of factorization, and this is difficult. In this way, the information is secure as long as the encryption scheme is change regularly.

Two original schemes for encrypting quantum information are the Bennett-Brassard 1984 scheme (commonly known as the BB84 scheme) or the Ekert protocol [24]. The latter harnesses a peculiar feature of quantum mechanical systems: quantum entanglement [25, 26]. All entangled pure quantum states violate an inequality called the Bell inequality. In Ekert protocol, this inequality is used to check that a shared quantum entangled state between two parties is not violated. Since entangled quantum states can produce quantum correlations that cannot be achieved classically, one could use this entangled property to generate common trash, i.e. a set of random correlated bits between the two parties called Alice and Bob (but could also be Ali and Bibi).

Why is this important? In classical information theory, it has been shown that a one-time pad consisting of random digits shared between two parties can serve as a secure key to lock and unlock messages. Such one-time pad is traditionally distributed between two parties through a trusted messenger. However, distribution of keys is highly insecure. The messenger could be captured or the one-time pad could be stolen. As an example, suppose we wish to transmit the secure message 001010111. Suppose also that Ali and Bibi shared a common list of trash digits 110101011 (key). Ali will encode the message as follows: he use the common trash to add to the message modulo 2; i.e. $001010111 \oplus 110101011$ to give 111111100. This encoded message does not reveal any information since any message encrypted with trash is really trash. When it arrives at Bibi’s site, Bibi uses the shared trash (key) and adds it to the encoded message modulo 2 again. This time, she gets: 111111100 (received message) $\oplus 110101011$ (key) gives 001010111 (desired message)! Mathematically, it hinges on the fact that $x \oplus x = 0$ regardless of the value of $x$, i.e. rubbish $\oplus$ rubbish is equivalent to adding a string of zeros. Naturally many
different variants of the original schemes have since been devised. Recent works have shown that the Ekert protocol can also be used for device-independent quantum cryptography in which the security of the communication does not depend on the need to trust the quantum devices used for the communication channel [27].

4. QUANTUM METROLOGY
Aside from quantum computation and communication, interest in quantum information processing has recently resulted in many advances in precision measurements. Precise clocks have many applications in research and the industry. Accurate clocks provided the resource needed for navigation, transport, network synchronization and even surveying through the Global Positioning System (GPS). Moreover, improvements in clock precision have deep implications for synchronization of quantum networks [28].

It recent years, it has been shown that the statistical scaling of errors can be surpassed with quantum entanglement. The typical experimental implementation is generally realized through a NOON state, which is really a superposition of \( N \) particles in one path (path A, say) and no particle in the other (path B) with the reverse case of no particles in path A and \( N \) particles in path B [29, 30]. The enhancement in precision can also be obtained with higher angular momentum states[31, 32].

5. CONCLUDING REMARKS
This article is never meant to be a comprehensive survey of the rich field of quantum information science. Nonetheless, it is hope that it provides a glimpse for people who would like to know something about the subject and it hopes perhaps to pique their curiosity regarding some of the fascinating features of this highly interdisciplinary science. One thing for sure: quantum information science has provide much impetus to research in physics, chemistry and recently biology and engineering. In the words of Serge Haroch: “It is hard to make predictions, especially about the future... (Attributed to Niels Bohr) ... but one thing is sure: without basic research, novel technologies cannot be invented... ...and the past teaches us that wonderful applications always emerge serendipitously from blue sky research”

6. ACKNOWLEDGMENTS
KLC would like to acknowledge the support of the Ministry of Education (Singapore) and the National Research Foundation of Singapore.

References
[1] Deutsch D 1985 Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences vol 400 (The Royal Society) pp 97–117
[2] Deutsch D, Barenco A and Ekert A 1995 Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences vol 449 (The Royal Society) pp 669–677
[3] Monroe C, Meekhof D, King B, Itano W and Wineland D 1995 Physical Review Letters 75 4714
[4] Schmidt-Kaler F, Häffner H, Riebe M, Gulde S, Lancaster G P, Deuschle T, Becher C, Roos C F, Eschner J and Blatt R 2003 Nature 422 408–411
[5] Gershenfeld N A and Chuang I L 1997 science 275 350–356
[6] Chang D E, Vandersypen L M and Steffen M 2001 Chemical physics letters 338 337–344
[7] O’Brien J L, Furusawa A and Vučković J 2009 Nature Photonics 3 687–695
[8] Nemoto K and Munro W J 2004 Physical review letters 93 250502
[9] Knill E, Laflamme R and Milburn G J 2001 nature 409 46–52
[10] O’Brien J L, Pryde G J, White A G, Ralph T C and Branning D 2003 Nature 426 264–267
[11] Rauschenbeutel A, Nogues G, Osnaghi S, Bertet P, Brune M, Raimond J and Haroche S 1999 Physical Review Letters 83 5166
[12] Sleator T and Weinfurter H 1995 Physical Review Letters 74 4087
[13] Wallraff A, Schuster D I, Blais A, Frunzio L, Huang R S, Majer J, Kumar S, Girvin S M and Schoelkopf R J 2004 Nature 431 162–167
[14] You J and Nori F 2006 arXiv preprint quant-ph/0601121
[15] Feynman R P 1982 International journal of theoretical physics 21 467–488
[16] Buluta I and Nori F 2009 Science 326 108–111
[17] Greiner M, Mandel O, Esslinger T, Hänsch T W and Bloch I 2002 nature 415 39–44
[18] Lewenstein M, Sanpera A, Ahufinger V, Damski B, Sen A and Sen U 2007 Advances in Physics 56 243–379
[19] Bloch I, Dalibard J and Zwerger W 2008 Reviews of Modern Physics 80 885
[20] Bloch I, Dalibard J and Nascimbène S 2012 Nature Physics 8 267–276
[21] Chang D, Gritsev V, Morigi G, Vuletić V, Lukin M and Demler E 2008 Nature Physics 4 884–889
[22] Angelakis D G, Huo M, Kyoseva E and Kwek L C 2011 Physical review letters 106 153601
[23] Angelakis D G, Huo M X, Chang D, Kwek L C and Korepin V 2013 Physical review letters 110 100502
[24] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Reviews of modern physics 74 145
[25] Ekert A K 1991 Physical review letters 67 661
[26] Jennewein T, Simon C, Weihs G, Weinfurter H and Zeilinger A 2000 Physical Review Letters 84 4729
[27] Acín A, Brunner N, Gisin N, Massar S, Pironio S and Scarani V 2007 Physical Review Letters 98 230501
[28] Kómá r P, Kessler E, Bishof M, Jiang L, Sørensen A, Ye J and Lukin M 2014 Nature Physics 10 582–587
[29] Giovanetti V, Lloyd S and Maccone L 2006 Physical review letters 96 010401
[30] Giovanetti V, Lloyd S and Maccone L 2011 Nature Photonics 5 222–229
[31] Napolitano M, Koschorreck M, Dubost B, Behbood N, Sewell R and Mitchell M W 2011 Nature 471 486–489
[32] D’Ambrosio V, Spagnolo N, Del Re L, Slussarenko S, Li Y, Kwek L C, Marrucci L, Walborn S P, Aolita L and Sciarrino F 2013 Nature communications 4