Artur Ekert

Personal Details

Born	19 September 1961 in Wroclaw, Poland.
Nationality:	British and Polish
Position:	Professor of Quantum Physics Mathematical Institute, University of Oxford, U.K. Director, Centre for Quantum Technologies Lee Kong Chian Centennial Professor, National University of Singapore
Contact:	artur.ekert@qubit.org
Website:	http://www.arturekert.org

Education and Degrees

1991	**D.Phil. Physics, Oxford.**
1988–1991	Graduate, Wolfson College, University of Oxford
1987–1988	Visiting student, University of Oxford and Imperial College, London.
1985	**M.Sc. Physics & Mathematics, Jagiellonian University, Cracow.**
1980–1985	Undegraduate, Jagiellonian University, Cracow.
1980	**Baccalaureate.**

Academic awards and distinctions

2007	The Royal Society Hughes Medal
2004	The European Union Descartes Prize (team award, project IST-QuComm)
1996	US Air Force “Windows on Science Award”
1995	The Institute of Physics Maxwell Medal & Prize
1988	Pirie-Reid Award, University of Oxford

Academic Appointments

2011–	Adjunct Professor, Tsinghua University, Beijing
2010–	Visiting Professor, National Institute of Informatics, Tokyo
2006–	Professor of Quantum Physics, Mathematical Institute, Oxford
2006–	Professorial Fellow, Merton College, Oxford
2006–	Lee Kong Chian Centennial Professor, National University of Singapore
2002–2006	Professorial Fellow, Kings College, Cambridge
2002–2006	Leigh-Trapnell Professor in Quantum Physics, University of Cambridge
2002–2005	Temasek Visiting Professor, Singapore
2000	Visiting Professor, NTT Basic Research Laboratories, Atsugi, Japan
1998–2002	Professor of Physics, University of Oxford
1998–2002	Fellow and Tutor in Physics, Keble College, Oxford
1994–1998	Research Fellow, Merton College, Oxford
1994–2001	Royal Society Howe Research Fellow
1993–1994	Visiting Professor, University of Innsbruck, Austria
1991–1994	Junior Research Fellow, Merton College, Oxford

Academic & Administrative Responsibilities

2015–	The Croucher Foundation: Board of Trustees
2013–	ETH Institute for Theoretical Studies (Zürich): Scientific Advisory Committee
2007–	Director of the Centre for Quantum Technologies, Singapore
2006–	Max Planck Institut für Quantenoptik (Garching): Advisory Board (Fachbeirat)
2002–2006	Cambridge Millennium Mathematics Project: Management Committee
2002–2006	Head of the Cambridge-MIT Collaboration in quantum information science
2002–2006	Director of the Centre for Quantum Computation, University of Cambridge
2001–2008	The Perimeter Institute (Canada): Scientific Advisory Board
2001–2002	University Examiner, Department of Physics, Oxford
1997–1998	Dean of Graduates, Merton College, Oxford
1997–1998	Tutor for Graduate Admissions, Merton College, Oxford
1993–2002	Founder of ”Quantum Cryptography & Computation Group”, Clarendon Laboratory, Oxford (from 1999 ”The Centre for Quantum Computation”)

Plenary, invited and tutorial lectures

Delivered over 500 invited lectures on various aspects of quantum physics and information science. These include plenary talks at conferences and annual meetings of physical societies, tutorial and technical lectures at universities and research centres in Europe, USA, Australia and Asia, e.g.

2015	World Science Festival, New York City
2014	John Bell Lecture Series, Belfast
2012	The 62nd Lindau Nobel Laureate Meeting
2011	American Physical Society March Meeting, Dallas
2007	Microsoft Technical Recognition Event, San Francisco
2006	National University of Singapore Centennial Lecture
2005	Plenary lecture at the Annual Meeting of the Deutsche Physikalische Gesellschaft (DPG) with all scientific sections and the Astronomical Society (AG) in the International Year of Physics (March 2005, Berlin)
2005	Frontiers in Mathematics Lectures, Texas A&M University
2003	Nicky Shaw Public Understanding of Mathematics Lecture, Cambridge
1998	Dublin Institute of Advanced Studies, 1998 Statutory Lecture
1996	US Air Force Academy, “Windows on Science Lecture, Colorado Springs

University teaching

Lectures: quantum mechanics, information theory, mathematical methods in physics, statistical physics, concepts in theoretical physics. Tutorials: quantum mechanics, statistical physics, kinetic theory. Supervised 19 Ph.D. students.

Consultancy

Advised several companies and government agencies, including Hewlett-Packard, Finmeccanica S.p.A., GCHQ (CESG) and the MITRE Corporation (JASON). Coauthor of the ARDA quantum information and technology roadmap (US Department of Energy, Los Alamos).

Updated June 18, 2015

Resumé of Achievements in Research

Artur Ekert is one of the pioneers of quantum information science. He is best known as the inventor of entanglement based quantum cryptography but he has also made many important contributions to the theory of quantum computation and other branches of quantum physics. Since his student days at Oxford he has been prominent in setting the agenda of, and leading, research efforts in the field. In his doctoral thesis (Oxford, 1991) he showed how quantum entanglement can be used to distribute cryptographic keys with perfect security. His subsequent paper on the use of Bell's inequalities as a statistical test for eavesdropping [1] has triggered an explosion of research efforts worldwide and continues to inspire new research directions. It is the most cited paper in the field (over 4200 citations according to the Web of Science) and was chosen by the editors of the Physical Review Letters as one of their "milestone letters", i.e. papers that made important contributions to physics, announced significant discoveries, or started new areas of research. In 2011 the American Physical Society devoted a special session of its annual March meeting to celebrating twenty years of entanglement-based quantum cryptography.

Apart from laying down the theoretical foundations for the use of entanglement in secure communication, Ekert has also contributed to the experimental development of the field. In collaboration with J. Rarity FRS and P. Tapster, his colleagues from the Defence Research Agency in Malvern (now QinetiQ), he set up the first experimental demonstration of entanglement-based key distribution, introducing several quantum optical techniques to the repertoire of cryptography [2]. This work has contributed greatly to making quantum cryptography a viable experimental and commercial proposition.

Ekert has subsequently made or participated in many of the most important advances in the field of broadly defined quantum information science, including the discovery of entanglement swapping [3], proposals for experimental realisations of quantum logic gates [4, 5], quantum state transfer in spin-chains [6], universality of quantum logic gates [7], distributed quantum computation [8], improved frequency standards [9] and decoherence free subspaces [10].

He is chiefly responsible for introducing the subject of quantum computation to the atomic and quantum optics community. In his, now famous, talk at the 1994 International Conference on Atomic Physics held in Boulder, Colorado, Ekert outlined how to make the most basic components of quantum computers – quantum logic gates – and thus inspired many physicists to work on the experimental realisations of quantum computation, (see, for example, D. Wineland's 2012 Nobel Lecture).

Ekert is a world-recognised ambassador of quantum information science and quantum technologies. He has delivered over 500 invited lectures on various aspects of quantum data processing. These include plenary talks at various conferences and annual meetings of physical societies, tutorial and technical lectures at universities and research centres in Europe, USA, Australia and Asia. In 1990 he established the world's first research group in quantum cryptography and computation (Clarendon Laboratory, Oxford). In 1997 he was one of the initiators and contributors to the EU Pathfinder project, which paved the way for subsequent European initiatives in quantum information science. In 2004 he helped to establish the US quantum information science and technology roadmap and in 2007 he set up a vibrant quantum technology research programme in Singapore. In Oxford and Cambridge he has supervised about twenty Ph.D. students and acted as a mentor to over thirty post-doctoral researchers, many of whom have subsequently made their own substantial contributions to the field. He was influential in shaping the UK early research in quantum information science, which led to both the UK having a leading role both in the early development of the field and its current strong standing.

There is no doubt that Artur Ekert has played a pivotal role in transforming the field of quantum information science from what was initially perceived to be merely a fringe pursuit into an area of vigorous and dynamic international activity.

Selected Highlights

Quantum Cryptography

Ekert is the inventor of entanglement-based quantum cryptography [1]. His 1991 paper on the subject generated a spate of new research that effectively established a vigorously active new area of physics and cryptology. More recent research has shown that his original key distribution scheme enables devices of unknown or dubious provenance, even those that are manufactured and controlled by adversaries, to be safely used for secure key distribution (device-independent cryptography). Moreover, security that is guaranteed by a certain type of correlations, no matter whether they are of quantum origin, does not rely on the validity of quantum theory. Thus if one day quantum theory is refuted and superseded by another theory that admits non-local correlations (violates Bell's inequalities) the Ekert key distribution scheme will still be secure. One should add here that Ekert's original idea has also non-cryptographic applications, e.g. testing and amplifying randomness (unpredictability) of quantum random bit generators.

His work with J. Rarity and P. Tapster from the Defence Research Agency in Malvern, which included the first experimental demonstration of entanglement-based key distribution [2], gave the Bell inequalities a tangible practical meaning! Addressing the security issues in noisy quantum channels, he has proposed quantum privacy amplification, which makes entanglement-based quantum crypto-systems operable and secure even over noisy quantum channels [11]. Quantum privacy amplification (entanglement purification) together with entanglement swapping, which he proposed in collaboration with A. Zeilinger, M. Horne and M. Żukowski [3], and the use of quantum repeaters, enables (in principle) the distribution of quantum entanglement, and hence cryptographic keys, over arbitrarily long distances.

Quantum Computation

Ekert has contributed several results ranging from mathematical analysis of quantum algorithms to proposals for experimental realisations of quantum logic gates.

Algorithms: A common pattern underpinning all known quantum algorithms can be identified when quantum computation is viewed as multi-particle interference. With R. Cleve, C. Macchiavello and M. Mosca, Ekert has developed and used this approach to review and to improve some of the existing quantum algorithms and to show how they are related to different instances of quantum phase estimation [12]. In collaboration with M. Mosca, he has also provided a unified mathematical picture of quantum algorithms in terms of group theory (searching for hidden subgroups) and described its connection with eigenvalue estimation on a quantum computer. The hidden subgroup problem also encompasses the problem of finding orders of elements in a group, of which Shor's celebrated factoring algorithm is a special case [13].

Quantum logic gates and networks: Ekert worked on the basic constituents of quantum computers, i.e. quantum logic gates and quantum Boolean networks, and he contributed to several advances in the field. In particular he proved that almost any quantum logic gate operating on two quantum bits is universal [7] (with D. Deutsch FRS and A. Barenco) and introduced the concept of distributed quantum computation over noisy channels [8] (with I. Cirac, S. Huelga, and C. Macchiavello).

Implementations: Though his focus has usually been on fundamental issues, Ekert has proposed several experimental implementations of the quantum controlled-NOT gate [4] (together with A. Barenco, D. Deutsch and R. Jozsa), including the idea of using the induced dipole-dipole coupling in an optically driven array of quantum dots as a suitable architecture for quantum processors. Although his array of quantum dots may never be used for quantum coherent computation, the idea alone stimulated researchers at HP Labs in Palo Alto (S. Williams and his colleagues) to design novel molecular processors for more conventional computation.

Quantum error correction and stabilising quantum computation

Extended quantum computation requires maintaining the coherence of a relatively large quantum system against corrupting environmental interactions. It will be necessary to incorporate error correction or stabilisation schemes to combat unwanted environmental influences known as decoherence. Together with D. Deutsch and A. Berthiaume, Ekert contributed to the development of the earliest recoherence scheme based on projections on symmetric subspaces [14]. Subsequently, he proposed "noiseless encoding" [10], which became later known as decoherence free subspaces. He also derived the Hamming and the Gilbert-Varshamov bounds for quantum analogues of linear error correcting codes. In search of new methods of error avoidance, he has proposed the implementation of a conditional Berry phase between two nuclear spins [5] (joint work with J. Jones, V. Vedral and G. Castagnoli). Combined with one-spin operations, this simple operation is a universal gate for quantum computation; any unitary transformation can be implemented with arbitrary precision using only one-spin operations and conditional phase shifts. Thus quantum geometrical phases can form the basis of any quantum computation. Moreover, as the induced conditional phase depends only on the geometry of the path executed by one of the spins, it is resilient to certain types of errors and offers the potential of a naturally fault-tolerant way of performing quantum computation. This work was followed by a paper in which he clarified the meaning of geometric phases for mixed quantum states.

Physics, mathematics and computation

Ekert has written several influential papers on the foundations of, and philosophical implications of, quantum physics. One of them is his paper with D. Deutsch and R. Luppachini [15] on the dependence of mathematical knowledge on our knowledge of physics. He has also studied the connections between the notion of mathematical proofs and the laws of physics, e.g. whether we can trust mathematical proofs performed by (quantum) machines when the proofs cannot be explicitly verified by humans. He has argued that we have to abandon the classical view of computation as an independent logical notion in favour of that of computation as a physical process. In his writings, be they popular or technical, he often advocates new kinds of knowledge and insights that the richness and intricacy of the quantum world can offer (e.g. in the special edition of Scientific American, Extreme Physics, May 2013).

Miscellaneous

Ekert has worked on many other topics, to mention only quantum state swapping, entanglement detection, optimal quantum state estimation and quantum state transfer. In collaboration with D. Bruss and C. Macchiavello, he established the best possible approximation to a universal quantum cloning machine [16]. The result is general and admits cloners that operate on mixed input states. His paper on purification of qubits [17] (joint work with J.I. Cirac and C. Macchiavello) led to the development of powerful group-theoretical methods for estimating spectra of density operators. Together with P. Horodecki he proposed an efficient way of detecting quantum entanglement [18]. He has also proposed several novel uses of quantum entanglement, most notably for the improvement of quantum frequency standards via prescribed entangled states [9], new methods for an efficient state transfer in spin-chains [6] and, more recently, a new model for decoherence-assisted energy transfer in biological systems [19].

Ekert has also been working with historians of science on the origin and evolution of the concept of randomness. Part of that project involved his work on G Cardano's role in the origins of probability and complex numbers, and resulted in several semi-popular papers.

His current research interests are focused on the nature of randomness, including quantum randomness amplification and randomness expansion. His recent paper on the subject (joint work with R. Renner) outlines the present status and the challenges in this new emerging field [20].

Artur Ekert's most significant 20 publications

[1] A.K. Ekert, "Quantum Cryptography Based on Bell Theorem", Physical Review Letters **67**, 661–663 (1991).

[2] A.K. Ekert, J.G. Rarity, P.R. Tapster and G.M. Palma, "Practical quantum cryptography based on 2-photon interferometry", Physical Review Letters **69**, 1293–1295 (1992).

[3] M. Żukowski, A. Zeilinger, M.A. Horne and A.K. Ekert, "Event-Ready-Detectors, Bell Experiment via Entanglement Swapping", Physical Review Letters **71**, 4287–4290 (1993).

[4] A. Barenco, D. Deutsch, A. Ekert and R. Jozsa, "Conditional quantum dynamics and logic gates", Physical Review Letters **74**, 4083–4086 (1995).

[5] J.A. Jones, V. Vedral, A. Ekert and G. Castagnoli, "Geometric quantum computation using nuclear magnetic resonance", Nature **403**, 869–871 (2000).

[6] M. Christandl, N. Datta, A. Ekert and A.J. Landahl, "Perfect state transfer in quantum spin networks", Physical Review Letters **92**, 187902 (2004).

[7] D. Deutsch, A. Barenco and A. Ekert, "Universality In Quantum Computation", Proceedings of the Royal Society A **449**, 669–677 (1995).

[8] J.I. Cirac, A.K. Ekert, S.F. Huelga and C. Macchiavello, "Distributed quantum computation over noisy channels", Physical Review A **59**, 4249–4254 (1999).

[9] S.F. Huelga, C. Macchiavello, T. Pellizzari, A.K. Ekert, M.B. Plenio and J.I. Cirac, "Improvement of frequency standards with quantum entanglement", Physical Review Letters **79**, 3865–3868 (1997).

[10] G.M. Palma, K.A. Suominen and A.K. Ekert, "Quantum computers and dissipation", Proceedings of the Royal Society A **452**, 567–584 (1996).

[11] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu and A. Sanpera, "Quantum privacy amplification and the security of quantum cryptography over noisy channels", Physical Review Letters **77**, 2818–2821 (1996).

[12] R. Cleve, A. Ekert, C. Macchiavello and M. Mosca, "Quantum algorithms revisited", Proceedings of the Royal Society A **454**, 339–354 (1998).

[13] M. Mosca and A. Ekert, "The hidden subgroup problem and eigenvalue estimation on a quantum computer", in Quantum Computing and Quantum Communications, Vol. 1509, edited by C Williams, Lecture Notes in Computer Science (1999), pp. 174–188.

[14] A. Barenco, A. Berthiaume, D. Deutsch, A. Ekert, R. Jozsa and C. Macchiavello, "Stabilization of quantum computations by symmetrization", SIAM Journal on Computing **26**, 1541–1557 (1997).

[15] D. Deutsch, A. Ekert, and R. Lupacchini, "Machines, logic and quantum physics", Bulletin of Symbolic Logic **6**, 265–283 (2000).

[16] D. Bruss, A. Ekert and C. Macchiavello, Optimal universal quantum cloning and state estimation, Physical Review Letters **81**, 2598–2601 (1998).

[17] J.I. Cirac, A.K. Ekert and C. Macchiavello, "Optimal purification of single qubits", Physical Review Letters **82**, 4344–4347 (1999).

[18] P. Horodecki and A. Ekert, "Method for direct detection of quantum entanglement" Physical Review Letters **89**, 127902 (2002).

[19] I. Sinayskiy, A. Marais, F. Petruccione and A. Ekert, "Decoherence-Assisted Transport in a Dimer System", Physical Review Letters **108**, 020602 (2012).

[20] A. Ekert and R. Renner, "The ultimate physical limits of privacy", Nature **507**, 443–447 (2014).