Scientific Report

First name / Family name	Colin Wilmott
Nationality	Irish
Name of the *Host Organisation*	Masaryk University
First Name / family name of the *Scientific Coordinator*	Jan Bouda
Period of the fellowship	01/11/2011 to 31/10/2012

I – SCIENTIFIC ACTIVITY DURING YOUR FELLOWSHIP

As part of the ERCIM fellowship scheme, I joined the quantum information science group at Masaryk University in Brno, Czech Republic. My research was in conjuction with group members Jan Bouda, Martin Plesch and Matej Pivoluska. Our research mainly followed the topic of research initially established at the beginning of my fellowship. We focused on the role of weak stochastic processes in various aspects of quantum cryptography. The work produced one publication in Phys. Rev. A. and preparations are under way for a second paper on the same topic. We also completed research concerned with quantum encryptions using weak randomness and we hope to submit soon. Additionally, we began new research on the topic of quantum secret sharing. Main highlights of the year include:

Journal Award
Journal: Journal of Physics A Mathematical and Theoretical
Date of award: December 2011
Award for one of the most outstanding publications of 2011. This prize was in recognition of my work on the geometry of quantum polytopes.

Conference Award
Conference: 12th Asian Conference on Quantum Information Science (AQIS '12)
Date of award: August 2012
Co-authored work with Bouda, Plesch and Pivoluska. We won the 1st prize award for the

conference's most outstanding contribution.

II – PUBLICATION(S) DURING YOUR FELLOWSHIP

Publication 1

Title: A construction of a generalized quantum SWAP gate (with P Wild)
Journal: Int. J. Quan. Info. 10 3 (2012)
DOI No: 10.1142/S0219749912500347
Abstract: The SWAP gate plays a central role in network designs for qubit quantum computation. However, there has been a view to generalize qubit quantum computing to higher dimensional quantum systems. In this paper we construct a generalized SWAP gate using only instances of the generalized controlled-NOT gate to cyclically permute the states of d qudits for d prime.

Publication 2

Title: Algorithm for characterizing stochastic local operations and classical communication classes of multiparticle entanglement (with D Bruß, O Gühne and H Kampermann)
Journal: Phys. Rev. A 86 032307 (2012)
DOI: 10.1103/PhysRevA.86.032307
Abstract: It is well known that the classification of pure multiparticle entangled states according to stochastic local operations leads to a natural classification of mixed states in terms of convex sets.We present a simple algorithmic procedure to prove that a quantum state lies within a given convex set. Our algorithm generalizes a recent algorithm for proving separability of quantum states [Barreiro et al., Nat. Phys. 6, 943 (2010)]. We give several examples which show the wide applicability of our approach. We also propose a procedure to determine a vicinity of a given quantum state which still belongs to the considered convex set.

Publication 3

Title: Weak randomness trounces the security of QKD (with J Bouda, M Pivoluska and M Plesch)
Journal: Phys. Rev. A 86, 062308 (2012)
DOI: 10.1103/PhysRevA.86.062308
Abstract: In usual security proofs of quantum protocols the adversary (Eve) is expected to have full control over any quantum communication between any communicating parties (Alice and Bob). Eve is also expected to have full access to an authenticated classical channel between Alice and Bob. Unconditional security against any attack by Eve can be proved even in the realistic setting of device and channel imperfection. In this paper we show that the security of quantum key distribution protocols is ruined if one allows Eve to possess a very limited access to the random sources used by Alice. Such knowledge should always be expected in realistic experimental conditions via different side channels.

Publication 4

Title:On a family of linear recurrences
Journal: Proc. Int. Conf. Mathematical Modelling in Physical Sciences – Journal of Physics: Conference Series 410 (2013) 012057
DOI: 10.1088/1742-6596/410/1/012057
Abstract: The theory of linear recurrences have many interesting and varied applications We concern ourselves with the family of linear recurrence relations a(j) = a(j−1) + a(j−d)

with the initial conditions a(0) = ... = a(d−1) = 1. We discuss the periodicity evaluation of such recurrences for prime powers d, and demonstrate that a key feature of our evaluation method relates to an instance of Shor's algorithm for factoring.

Publications Pending
Title: Towards an optimal generalised quantum SWAP gate
Submitted: Quantum Inf. Process – 15 pages

Title: On a family of dthorder linear recurrence relations
Submitted: Computational Science & Discovery – 10 pages

Title: Quantum encryptions using weak randomness (with J Bouda, M Pivoluska and M Plesch) In preparation

Title: Quantum Secret Sharing Designs (with J Bouda, M Pivoluska and M Plesch)
In preparation

III – ATTENDED SEMINARS, WORKSHOPS, CONFERENCES

SEMINARS GIVEN:
Seminar Title: On the identification of SLOCC classes of multiparticle entanglement
Invited seminar.
Date: November 2012
Location: QuIC, Université Libre de Bruxelles

Seminar Title: Convex geometry, inequalities and partial orders (As part of the ERCIM research exchange programme)
Date: October 2012
Location: Faculty of Mathematics and Physics, Charles University, Prague

Seminar Title: SLOCC classes of multiparticle entanglement
Date: October 2012
Location: Faculty of Informatics, Masaryk University, Brno

Seminar Title: Combinatorial designs of quantum circuits (As part of the ERCIM research exchange programme)
Date: March 2012
Location: Department of Mathematics, University of Warsaw

Seminar Title: Characterizing multiparticle entanglement properties via convex polytopes
Invited seminar.
Date: February 2012
Location: School of Mathematics, NUI Galway

Seminar Title: Sign permutation polytopes, weak majorization & multiparticle entanglement
Date: February 2012

Location: Institute of Theoretical Physics, University of Vienna

CONFERENCE PARTICIPATION:
Conference Talk: On a family of linear recurrences
Date: October 2012
Location: International Conference on Mathematical Modelling in the Physical Sciences, Budapest

WORKSHOP PARTICIPATION:
Workshop Poster: Deriving a basis for the set of bounded operators on a d-dimensional Hilbert space
Date: June 2012
Location: 9th Central European Quantum Information Processing Workshop, Smolenice, Slovakia

IV – RESEARCH EXCHANGE PROGRAMME (REP)

First Exchange Visit:
Geometry Group
Faculty of Mathematics
University of Warsaw
Warsaw, Poland
Date: March 2012
Local scientific coordinator: Daniel Adamiak
Local contacts in Mathematics: Tomasz Zukowski and Maria Moszynska

As part of the ERCIM research exchange programme, I visited the Faculty of Mathematics at the University of Warsaw. My contact here was Professor Moszyska who gave me a very big warm welcome on my arrival. Maria was very kind and ensured my visit was smoothly. I met with a large section of the people from the geometry group, discussed my research and I also presented my work on quantum polytopes at their seminar series.

Second Exchange Visit:
Faculty of Mathematics
Charles University
Prague, Czech Republic
Date: October 2012
Local scientific coordinator: Vaclav Matyas
Local contacts in Mathematics: Jan Kratochvil

For my second ERCIM research exchange stay, I visited the Faculty of Mathematics at Charles University in Prague. I met with Professor Kratochvil and his research group where I discussed some of my work.