A. CURRICULUM VITAE

1. Name: Elham Kashefi

2. School: Informatics

3. College: Science and Engineering

4. Date of first appointment in The University of Edinburgh: 31/09/2007

5. Date of promotion in The University of Edinburgh: April 2012 (Lecturer to Reader)

6. Career

Oct 15 – Oct 2020	**Engineering and Physical Sciences Research Council, UK** Established Career Research Fellow
Jan 15 – Jan 2020	**NQIT EPSRC National Network of Quantum Technology Hubs, UK** Associate Director of Applications
Sept 14 – Present	**CNRS Laboratoire Traitement et Communication de l'Information, France** CR1 Researcher
Aug 12 – Present	**School of Informatics, University of Edinburgh, UK** Reader (On 50% leave since Oct 2015)
Apr 08 – Aug 12	**School of Informatics, University of Edinburgh, UK** Lecturer (on maternity leave from 15/08/2011 till 4/12/2011)
2011 – Present	**Telecome ParisTech, CNRS, France** Maitre de Conférences Associé (Affiliated Associate Professor)
Apr 08 – Apr 2013	**Engineering and Physical Sciences Research Council, UK** Advanced Research Fellow
Sept 07 – Apr 08	**Laboratoire d'Informatique de Grenoble, CNRS, France** CR1 Researcher
June 03 – Sep 07	**Christ Church College and Computing Laboratory, Oxford, UK** Junior Research Fellow in Quantum Information Theory
March 06 – March 07	**Massachusetts Institute of Technology, US** Visiting Scientist, Department of Theoretical Physics
Jan 05 – Jan 06	**Institute for Quantum Computing, University of Waterloo, Canada** Post-doctoral Fellow, Department of Mathematics
1999 – 2003	**Imperial College, London, UK** Research Assistant in Programming Language Theory Group (Computing) & Quantum Information and Optics Group (Physics)

7. University Education and Degrees

1999 – June 03	**Imperial College, London, England** PhD in Computer Science, Supervisor: Prof. Vlatko Vedral Thesis Title: *Complexity Analysis and Semantics for Quantum Computing*
1996 – 1998	**Sharif University of Technology, Tehran, Iran** MSc in Applied Mathematics, Supervisor: Prof. Ebad Mahmoodian Thesis Title: *Combinatorial Game Theory*
1991 – 1996	**Sharif University of Technology, Tehran, Iran** BSc in Applied Mathematics and Computer Science

8. Teaching Experience

- Invited Lecturer at Formal Methods for Analysis of Computer Systems, IPM Iran, 2016
- Co-Lecturer at the Parisian Master of Research in Computer Science, 2016
- Invited Lecturer for Quantum Simulation and Computation Summer School, Sweden, 2015
- Invited Lecturer for Quantum Physics and Computer Science School, France, 2014
- Lecturer (full term) for Introduction to Quantum Computing (Level 9 and 10), University of Edinburgh, 2013 (*Favourable Student Feedback, two students took my projects afterward*)
- Invited Lecturer for Quantum Complexity, Imperial College, Doctoral Training Center, 2011
- Invited Lecturer for the10th International School on Formal Methods for the Design of Computer, Communication and Software Systems, Italy, 2010
- Lecturer (full term) for the LFCS Advanced Course on Models of Quantum Computing University of Edinburgh, 2009 (*two students took my projects afterward*)
- Invited Lecturer for the International Summer School on Quantum Information, Iran, 2008
- Lecturer for Quantum Information Theory, Christ Church College, Oxford University, 2006
- Invited Lecturer for Models of Computing, University of Tokyo, Japan, 2005
- Invited Lecturer for Quantum, Atomic and Molecular Physics School, Open University, 2003

- Committee member of the restructuring the Quantum Information courses at Telecom ParisTech, France, 2015-2016

- Founder of a 5 years international teaching program for Advanced Quantum Cryptography sponsored by Telecome ParisTech and my EPSRC established Career Fellowship as part of the CNRS-Telecom ParisTech-Edinburgh joint quantum lab to be commencing in June 2016

- Co-Author of the following book chapters
  standard text book in teaching advance cources on quantum formal methods

    - Measurement-based and Universal Blind Quantum Computation, A. Broadbent, J. Fitzsimons, E. Kashefi, In Formal Methods for Quantitative Aspects of Programming Languages, Edited by A. Aldini, M. Bernardo, A. Di Pierro, H. Wiklicky, LNCS 6154, Springer, 2010.
    - Extended Measurement Calculus, V. Danos, E. Kashefi, P. Panangaden, S. Perdrix, In Semantic Techniques in Quantum Computation, Edited by S. Gay, I. Mackie, Cambridge University Press, 2009.

9/12. Research Supervisions

- Post-Doctoral research

  - A. Pappa, Quantum Secure multi-party Computation, 2015 - 2017
    (NQIT Quantum Hub funding)
  - P.Wallden, Practical Verification, 2014 - 2016
    (Informatics Teaching Associate)
  - V. Dunjko, Hybrid Classical-Quantum Computing, College EPSRC fellowship, 2012 - 13
    (Now PDR at Innsbruck University)
  - T. Morimae, AKLT Blind Computing, SICSA and Japanese fellowship, 2011
    (Now Assist. Prof. at Gunma University Japan)

- PhD students

  - D. Mills, Quantum Simulation, Edinburgh, 2015 - Present
    (CDT in Pervasive Parallelism)
  - A. Gheorghiu, Practical Quantum Verification, Edinburgh, 2014 - Present
    (Best student paper award in Quantum Cryptography Conference 2015)
  - T. Kapourniotis, Efficiency and adaptivity of quantum verification, Edinburgh, 2012 – to be submitted in October 2015
    (Awarded a post-doctoral position at the university of Warwick 2016)
  - Ph.D Thesis on Quantum Parallel Computing, E. Pius, Edinburgh, 2010 - 2014
    (Now senior software engineer at ION geophysical)
  - Ph.D Thesis, Ideal quantum protocols in the non-ideal physical world, V. Dunjko, Edinburgh joint with Heriot-Watt , 2009 – 2012
    (Now PDR at Innsbruck University)

- Master students

  - Luka Music, Optimization Techniques for UBQC, Telecom ParisTech, 2015
    (Obtained the top mark in the group)
  - A. Gheorghiu, Entanglement and Verification, Edinburgh, 2014
    (Final short list for the VCLA outstanding master thesis award)
  - L. Disilvestro, Topological MBQC, Edinburgh, 2013
    (PhD student at TelecomParis Tech)
  - T. Kapourniotis, Blind Quantum Computing Protocols, Edinburgh, 2012
    (Awarded the Scotland MSc scholarship)
  - E. Pius, Quantum Parallelism, Edinburgh, 2010
  - F. Cipcigan, Diagnosing Optical Implementations of QC, Edinburgh, 2010
    (The final three for the Europe Science and Technology student of the year award)
  - Michael Crogan, Adiabatic Quantum Computing, Oxford University, 2006

- Undergrad students

  - 4th year Project, MBQC simulator, M. Marinov, University of Edinburgh, 2012
    (Nominated for the best project)
  - 4th year Project on Distributed Blind Quantum Computing, P. Fulop, Edinburgh, 2014
    (Top performance medal in BSc CS & Physics) (Now technology analyst at J.P. Morgan)
  - Summer Project, Topological Quantum Computing, L. Disilvestro, Edinburgh, 2013
  - Summer Project, Match gates MBQC, F. Cipcigan, Edinburgh, 2010
  - Summer Project on Quantum Random Walk, Lana Sheridan, Oxford University, 2005

10. Major Research Interests

- **Models of Quantum Computing**. Kashefi has explored the potential of quantum information theory from its formal and foundational aspects to actual cryptographic experiments. She has jointly developed the rigorous mathematical model underlying the measurement-based quantum computing [1, 2, 3, 4] and information flow analysis [5, 6, 7, 8] paving the road for wider access to such models among different sub-disciplines within computer science [9, 10, 11, 12, 13] (more than 600 joint citations).

- **Quantum Cryptography.** Kashefi has jointly invented the new cryptographic protocol of universal blind quantum computing (UBQC), demonstrating for the first time the possibility of preserving the privacy of computation using quantum properties [14, 15, 16, 17]. The UBQC has received strong praise (more than 200 joint citations) in the international quantum community as one of the major breakthroughs of the last decade (Vazirani QIP 2010, Aaronson Shtetl-Optimized 2011, Vedral Physics Today 2012, Zeilinger QCMC 2012).

- **Experimental Demonstration.** In collaboration with Prof. Walther's experimental lab in Vienna, Kashefi has adapted her theoretical work to the optical implementation [15]. Within a week of the publication of the Science paper, more than 50 articles appeared in the international media (including BBC) describing the work as achieving secure quantum cloud computing for the first time. This has set a new strategic dimension in her research to lead the work from theory [18] to the lab [19] and further to actual business development [20]. An end-to-end trend that she has been mastering since with other experimental labs [21]. In her recent collaboration with Walmsley's experimental lab in Oxford, she explored a hybrid quantum-classical approach where coherence can be used as a tool for secure delegated classical computation.

- **Quantum Verification.** A pressing challenge facing any kind of complex system and in particular the emerging quantum technology, is practical verification. Kashefi has jointly developed a new approach for testing the correctness of any delegated quantum computing based on the ability to compute with encrypted data, while hiding the underlying function. She has demonstrated, theoretically [22] and experimentally [23], that measurement of the randomly prepared single qubits, encrypted from the actual computation, leads to an efficient quantum certification. After her Nature Physics publication, various media (including a live BBC interview), praised the result as a quantum leap in bringing quantum technology closer to reality. She has since been at the forefront of quantum verification, developing a spectrum of various tests using technology available in quantum labs across the world [24, 25, 26].

References

[1] Danos, Kashefi, and Panangaden. Phys. Rev. A (2005)
[2] Danos, Kashefi, and Panangaden. ICALP (2006)
[3] Danos, Kashefi, and Panangaden, J. ACM (2007)
[4] Danos, Kashefi, Panangaden, and Perdrix. Semantic Techniques in Quantum Computation (2009)
[5] Danos and Kashefi. Phys. Rev. A (2006)
[6] Browne, Kashefi, Mhalla, and Perdrix. New J. Phys. (2007)
[7] Kashefi, Markham, Mhalla, and Perdrix. EPTCS (2009)
[8] Markham and Kashefi. In Horizons of the Mind. A Tribute to Prakash Panangaden. Springer (2014)
[9] Danos, d'Hondt, Kashefi, and Panangaden. QPL (2005)
[10] Broadbent and Kashefi. J. TCS (2009)
[11] Kashefi and et.al. MFPS (2009)
[12] Browne, Kashefi, and Perdrix. TQC (2010)
[13] Silva, Galvao, and Kashefi. Phys. Rev. A (2011)
[14] Broadbent, Fitzsimons, and Kashefi. FOCS (2009)
[15] Barz, Kashefi, Broadbent, Fitzsimons, Zeilinger, and Walther, Science (2012)
[16] Dunjko, Kashefi, and Leverrier. Phys. Rev. Lett. (2012)
[17] Morimae, Dunjko, and Kashefi. J. QIC (2015)

[18] Dunjko, Kapourniotis, and Kashefi. J. QIC (2015)
[19] Barz, Dunjko, Schlederer, Moore, Kashefi, and Walmsley, arXiv:1501.06730, (2015)
[20] UK Patent Application No 1402599.3, Quantum Enhanced Secure Delegated Computing, 2014
[21] Soudagar, Xing, Kashefi, Godbout, and Steinberg, Frontiers in Optics (2011)
[22] Fitzsimons and Kashefi. arXiv:1203.5217v1 (2012)
[23] Barz, Fitzsimons, Kashefi, and Walther, Nature Physics (2013)
[24] Kapourniotis, Kashefi, and Datta TQC (2014)
[25] Gheorghiu1, Kashefi, and Wallden. New J. Phys (2015)
[26] Dunjko, Kapourniotis, and Kashefi. AQISC (2015)

11. Research Grants

- EPSRC Established Career Fellowship, 2015 - 2020 (PI)
  Title: Verification of Quantum Technology
  Total value to UoE £1.2M, 50% PI time + 11 years PDR

- EPSRC Quantum Technology Hub, 2014 – 2019 (co PI and Associate Director)
  Title: Networked Quantum Information Technology
  Total of 38M, my share is 20% PI time + 5 years PDR, Total value to UoE £600K

- EPSRC Advanced Research Fellowship, 2008 - 2013 (PI)
  Title: Measurement-based quantum computing and its relation to other quantum models
  Total value to UoE £400K, 100% PI time

- Royal Academy of Engineering Distinguished Visiting Fellowship 2008 (PI)
- The Carnegie Trust for the Quantum Information Scotland (QUISCO) Network (co-PI)
- The Strategic French (CNRS) - Japanese (JST) Cooperative Program on “Quantum Computation: Theory and Feasibility” (co-PI)

13/15/17/18. Knowledge Exchange and Impact

- Submitted four papers at the last REF2014
- Editorial board for the Journal of Frontiers in ICT, since 2014
- Co-Founder of Quantum Information Scotland Network 2008 (now active partners in all Quantum Technology hubs)
- Co-Founder of Quantum Information Oxford University and Imperial College Network, 2003

- <u>Panel Invitaitons</u>

    - Expert Panel Member for the Workshop for Quantum Repeaters and Networks (declined due to overlap with other conference invitation) 2015
    - Speaker and Panel Expert for the GCHQ scoping meeting on Post-Quantum Research, Identifying Future Challenges and Directions, Turning Gateway to Mathematics, Cambridge, May and September 2014
    - EuroScience Open Forum (A new era of quantum mechanics), Denmark, 2014
    - Expert evaluator and Jury panel member for the Austrian R&D funding programme ICT of the Future, 2014
    - External Member for Interview Panel for a Chair Position at the Heriot-Watt University 2013
    - External Member for Interview Panel for a Lecturer Position at the Bristol University 2013
    - EPSRC Quantum Technology Workshop, scoping meeting, London, UK, 2013

- Directing the Industrial Partnership

    - Lockheed Martin (Initially approved but remained pending due to the lack of an agreement on the background IP negotiation)
    - BAE, Google, Keysight, IBM, PureLiFi (partners in the EPSRC Quantum Tech Fellowship with various “in kind” contribution)
    - Member of the Li-Fi R&D Centre Edinburgh
    - Quantum consultant for Baillie Gifford and Nordic Clou
- Outreach Activities

    - Invited Lecturer for The Times Cheltenham Science Festival, 2015
    - Live BBC Scotland Interview on quantum verification, 2014
    - Invited Lecturer for The Women in Science and Engineering Workshop, 2013
    - Invited Lecturer for Science group for University of the Third age, 2012
    - Athena SWAN Strategy Committee, 2013
    - Invited Lecturer for Cambridge Scientific Society Public Lecture, 2010
    - Invited Lecturer for the early career development and EPSRC grant application training course, Edinburgh, 2009

14. Academic Leadership and Management

- Managing board member of the Networked Quantum Information Technology (NQIT) Hub since 2014 (the only computer scientist and the only female with a directorial position within the EPSRC £120M investment in UK National Quantum Technology Programme)

- NQIT Associate director in charge of Quantum Applications development overseeing four work-packages with 5 PIs and 6 PDRs

- Founder of Telecom ParisTech - Informatics cooperation initiative since 2012 to be expanded to a joint CNRS Lab between LTCI-Informatics in 2016

15. Membership of Committees

- Program Committee of the 22nd Workshop on Logic, Language, Information and Computation (WOLLIC 2015)
- Program Committee of the 10th Conferance on Computability in Europe (CiE 2014)
- Program Committee of the XVII Conference on Quantum Information Processing (QIP 2014)
- Chair of the workshop on Parallel Quantum Computing (ParQ 2013)
- Organising committee for the Quantum Theory - Experiment Workshop at the International Institute of Physics, Brazil, 2013
- Co-Chair of the seventh Workshop on Developments in Computational Models (DCM 2011)
- Program Committee of the Theory of Quantum Computation, Communication and Cryptography (TQC, 2010 and 2011)
- Program Committee of the International Iran Conference on Quantum Information (IICQI-2010, 2012, 2014 and 2016)
- Organizing Committee of the First Quantum Information Paris (QUPA) - Quantum Information Scotland (QUISCO) network meeting
- Organizing Chair and Program Committee member of the sixth Workshop on Developments in Computational Models (DCM 2010)

16. Appointments as external examiner

- Itoop Vergheese Puthoor, University of Glasgow, Ph.D in Physics, December 2014
- Nick Papanikolaou, University of Warwick, Ph.D in Computer Science, July 2009
- Le Quoc Cuong, Telecom ParisTech, Ph.D. in Computer Science, August 2009
- Dang Minh Dung,Telecom ParisTech, Ph.D. in Computer Science, July 2008

19. Membership of Society

- Member of the international quantum institutions (PCQC - France, CQIQC - Canada)
- Elected member of the Young Academy of Scotland - Royal Society of Edinburgh, 2011
- Elected member of Engineering and Physical Sciences Research Council College, 2012

20. Items of esteem (Invited Speaker)

- Major Conference and Workshops

  - The International Conference on Quantum Communication, Measurement and Computing (QCMC), Singapore, 2016
  - UK National Quantum Technology Conference, Oxford, 2015
  - EACSL Annual Conference on Computer Science Logic (CSL), Germany, 2015
  - 7th Conference on Reversible Computation (RC), France, 2015
  - Trustworthy Quantum Information, USA, 2015
  - Bristol Quantum Information Technologies Workshop, 2015
  - Dagsthel Workshop on Challenges and Trends in Probabilistic Programming, 2015
  - EuroScience Open Forum (A new era of quantum mechanics), Denmark, 2014
  - The Mathematical Foundations of Programming Semantics (MFPS), US, 2014
  - OSA Quantum Information and Measurement Conference (QIM), Germany, 2014
  - Quantum Games and Protocols, Simons Institutes for Theory of Computing, US, 2014
  - Nordic Cloud and Mobile Security Forum, Sweden, 2013
  - Colloquium Jacques Morgenstern, INRIA Sophia Antipolis, France, 2013
  - Debating Conference on Quantum Information and Computing, French Academy of Sciences, France, 2013
  - IOP Topical Research Meetings on Physics, UK, 2012
  - Turing Research Symposium, Royal Society of Edinburgh, UK, 2012
  - Logic and interactions CRIM, Marseille, France, 2012
  - Isaac Newton Institute workshop on "The Incomputable", UK, 2012
  - Computability in Europe Conference (CiE), Bulgaria, 2011
  - Dagstuhl Workshop on Quantum Cryptanalysis, Germany, 2011
  - The 17th Central European Workshop on Quantum Optics (CEWOO), UK, 2010
  - Physics Colloquia at the Heriot Watt University, UK, 2010
  - The International Conference on Quantum Information and Technology, Japan, 2009
  - Studia Logica International Conference, Belguim, 2009
  - Paraty International Quantum Information Workshop and School, Brazil, 2007
  - The International Iran Conference on Quantum Information (IICQI), Iran, 2007
  - Workshop on Theory of Quantum Computation, Communication, and Cryptography (TQC), Japan, 2006
  - The International Conference on Quantum Communication, Measurement and Computing (QCMC), US, 2002
  - International Conference on Computability and Complexity in Analysis (CCA), Germany and US, 2001, 2002 and 2003

- Other International Workshops

    - EC3 Colombian Quantum Computing Meeting, Colombia, May 2015
    - Post-Quantum Research, Identifying Future Challenges and Directions, Turning Gateway to Mathematics, Cambridge, UK, May and September 2014
    - Conference in honour of Prakash Panangaden 60th birthday, Oxford, UK, May 2014
    - Quantum Logic Workshop, Amsterdam, Netherlands, April 2014
    - Lec Probabilismes, Cournot Centre, Paris, France, 2014
    - Quo Vadis Quantum Physics? The International Institute of Physics, Brazil, 2013
    - Royal Society International Scientific Seminar, Milton Keynes, UK, 2012
    - Quantum Information Science Workshop, Oxford, UK, 2012
    - Quantum Information and Graph Theory (Emerging Connections), Canada, 2011
    - McGill-Bellairs Research Institute, Information Theory and Security Workshop, 2010
    - Workshop on Distributed Quantum Computing, Italy, 2010
    - Workshop on "Foundational Structures for Quantum Information", Austria, 2008
    - CATS, KETS AND CLOISTERS Workshop, UK, 2006
    - Quantum Information, Computation and Logic Workshop, Canada, 2005
    - Workshop on the Thermodynamics of Entanglement, UK, 2004
    - McGill-Bellairs Research Institute, Semantical Methods in QC Workshop, 2004

- National Invitations

    - University of Oxford, Cloud Security, 2016
    - GCHQ, Quantum Verification, 2015
    - University of Bristol, Quantum-enhanced Secure Computing, 2014
    - University of Lancaster, Quantum Parallelism, 2013
    - University of Strathclyde, Quantum Cryptography, 2012
    - Imperial College, Can we trust a quantum computer, 2011
    - University of Birmingham, Verification of Quantum Computing, 2011
    - University of Nottingham, Verification of Quantum Mechanics, 2010
    - University of Leeds, Universal Blind Quantum Computing, 2010
    - University College London, Blind Quantum Computing, 2009
    - University of Bristol, Computing without Trusting, 2008
    - University of Glasgow, Quantum Protocol, 2008
    - University of Birmingham, Formalising Physical Computations, 2007
    - Leeds University, One-way and no other way, 2004

- Invited Long-Term Visiting Scientist

    - Simons Institute (Logical Structures in Computation), US, 2016
    - Center for Quantum Technology, Singapore, 2015
    - Simons Institute (Quantum Hamiltonian Complexity), US, 2014
    - Isaac Newton (New Mathematical Directions for Quantum Information), 2013
    - Laboratoire PPS, Universite Paris Diderot, France, 2013
    - The Photonic Quantum Computation & Simulation Center, University of Vienna, 2012
    - The centre for Quantum Computation and Intelligent Systems, University of Technology Sydney, 2011
    - Osaka Prefecture University, Japan, 2011
    - The Quantum Information Team at Telecom ParisTech, France, 2011, 2012
    - The Center for Extreme Quantum Information Technology, MIT, 2010
    - The Quantum Information Sciences group at NII, Japan, 2009
    - The Instituto de Física of the Universidade Federal Fluminense, Rio de Janeiro state, Brazil, 2009

B. LIST of PUBLICATIONS

I have papers in high profile publishing venues of several fields. My 2007 paper on “Measurement Calculus” was published in the *Journal of ACM* - regarded as the top venue for computer science articles. My 2009 paper on “Universal Blind Quantum Computing” was published at *FOCS*, the premiere conference in algorithms and complexity. I led the theoretical development for the experimental demonstration of my protocols published in *Science* 2012 and *Nature Physics* 2013. My publication list also includes significant papers in *Phys. Rev. Lett*. and the *New Journal of Physics* that are highly regarded in the Physics community. On the computer science side, I have publications in the high impact journal of *Quantum Information and Computation*. Note that high-quality conferences in this field (e.g. *ICALP, TQC, FOCS, QCrypt, AQISC* that I have published in) have a rigorous and very competitive refereed selection process based on submitting full papers. As requested, an asterisk denotes lead author (or equal contribution of the PI). Author order is not significant in computer science community as we generally use alphabetical order. For collaborations with experimental physicists sometimes a different rule is agreed, where the theoretical leader of the project either appears as the second author or next to the last.

Books Chapter

- D. Markham and E.Kashefi, Entanglement, Flow and Classical Simulatability in Measurement Based Quantum Computation, In F. van Breugel et al., editor, Panangaden Festschrift, 8464, LNCS, 2014.

- * Measurement-based and Universal Blind Quantum Computation, A. Broadbent, J. Fitzsimons, E. Kashefi, In Formal Methods for Quantitative Aspects of Programming Languages, Edited by A. Aldini, M. Bernardo, A. Di Pierro, H. Wiklicky, LNCS 6154, Springer, 2010.

- Proceedings Sixth Workshop on Developments in Computational Models: Causality, Computation, and Physics, Edited by S. Barry Cooper, E. Kashefi and P. Panangaden, EPTCS 26, 2010.

- * Extended Measurement Calculus, V. Danos, E. Kashefi, P. Panangaden, S. Perdrix, In Semantic Techniques in Quantum Computation, Edited by S. Gay, I. Mackie, Cambridge University Press, 2009.

Refereed Journal Articles

- * V. Dunjko, T. Kapourniotis and E. Kashefi, Quantum-enhanced Secure Delegated Classical Computing, *Journal of Quantum Information and Computation,* 2015

- Cheorghiu, E. Kashefi, P. Wallden, Robustness and device independence of verifiable blind quantum computing, *New Journal of Physics*, 2015

- *R. Dias da Silva, E. Pius and E. Kashefi, Global Quantum Circuit Optimization, *Journal of Quantum Information and Computation,* 2015

- *T. Morimae, V. Dunjko and E. Kashefi, Ground state blind quantum computation on AKLT state, *Journal of Quantum Information and Computation*, 2015

- *S. Barz, J. Fitzsimons, E. Kashefi and P. Walther, Experimental verification of quantum computations, *Nature Physics*, 2013

- V. Dunjko, E. Kashefi and A, Leverrier, Universal Blind Quantum Computing with coherent states, *Phys. Rev. Lett*. 2012

- *S. Barz, E. Kashefi, A. Broadbent, J. Fitzsimons, A. Zeilinger, P. Walther, Experimental Realization of Blind Quantum Computing, *Science*, 2012

- V. Dunjko and E. Kashefi, Extended Phase Map Decomposition, Mathematical Structures in Computer Science, 2012

- *R. D. da Silva, E. F. Galvao, E. Kashefi, Closed timelike curves in measurement-based quantum computation, *Phys. Rev. A*, 2011

- *J. Anders, E. Andersson, D. E Browne, E. Kashefi, D. K Oi, Ancilla-driven quantum computation with twisted graph states, *Journal of Theoretical Computer Science*, 2011

- J. Anders, D. K. L. Oi, E. Kashefi, D. E. Browne, and E. Andersson, Ancilla-driven universal quantum computation, *Phys. Rev. A*, 2010

- *Broadbent, E. Kashefi, Parallelizing Quantum Circuits, *Journal of Theoretical Computer Science*, 2009

- *D. Browne, E. Kashefi, M. Mhalla and S. Perdrix, Generalized Flow and Determinism for the Measurement-based Quantum Computing, *New Journal of Physics*, 2007

- *E. Kashefi and I. Kerenidis, Statistical Zero Knowledge and quantum one-way functions, *Journal of Theoretical Computer Science*, 2007

- *M. Silva, V. Danos, E. Kashefi, and H. Olivier, A direct approach to fault-tolerance in measurement-based quantum computation via teleportation, *New Journal of Physics*, 2007

- *V. Danos, E. Kashefi, P. Panangaden, The Measurement Calculus, *Journal of ACM*, 2007

- *V. Danos and E. Kashefi, Determinism in the one-way model, *Phys. Rev. A*., 2006

- *V. Danos, E. Kashefi, and P. Panangaden, Robust and parsimonious realisations of unitaries in the one-way model*, Phys. Rev. A.*, 2005

- V. Vedral and E. Kashefi, Uniqueness of entanglement measure and thermodynamics, *Phys. Rev. Lett.*, 2002

- *E. Kashefi, H. Nishimura, and V. Vedral, On quantum one-way permutations, *Journal of Quantum Information and Computation*, 2002

- *E. Kashefi, A. Kent, V. Vedral, and K. Banaszek, A comparison of quantum oracles, *Phys. Rev. A*, 2002

Refereed Conferences and Workshops Articles

- T. Kapourniotis, V. Dunjko and E. Kashefi, On optimising quantum communications in verifiable quantum computing, *the 15th Asian Quantum Information Science Conference*, Korea, AQIS2015

- Cheorghiu, E. Kashefi, P. Wallden, Robustness and device independence of verifiable blind quantum computing, *the Quantum Cryptography Workshop*, Japan, QCrypt2015

- *T. Kapourniotis, E. Kashefi and A. Datta, Verified Delegated Quantum Computing with One Pure Qubit, *the 9th Conference on the Theory of Quantum Computation, Communication and Cryptography*, Singapore, TQC2014

- Y. Soudagar, X. Xing, E. Kashefi, N. Godbout, A. Steinberg, Experimental Demonstration of a 4-qubit Loop Graph for One-way QC*, Frontiers in Optics*, US, FiO/LS2011

- V. Dunjko and E. Kashefi, Algebraic Characterization of One-way Patterns, *the Sixth Workshop on Developments in Computational Models*, Edinburgh, DCM2010

- *D. E. Browne, E. Kashefi, S. Perdrix, Computational depth complexity of measurement-based quantum computation, *the fifth Conference on the Theory of Quantum Computation, Communication and Cryptography*, Leeds, TQC2010

- *S. Salek, F. Seifan, E. Kashefi, Programmable Hamiltonian for One-way Patterns, *the 6th International Workshop on Quantum Physics and Logic*, Oxford, QPL2009

- *E. Kashefi, D. Markham, M. Mhalla, S. Perdrix, Information Flow in Secret Sharing Protocols, *the 5th Workshop on Developments in Computational Models*, Greece, DCM2009

- *E. Kashefi, D. K. L. Oi, D. E. Browne, J. Anders, E. Andersson, Twisted graph states for ancilla-driven quantum computation, *the 25th Conference on the Mathematical Foundations of Programming Semantics*, Oxford, MFPS2009

- *Broadbent, J. Fitzsimons, E. Kashefi, Universal blind quantum computation, the 50th Annual Symposium on Foundations of Computer Science, US, FOCS2009

- N. de Beaudrap, V. Danos, E. Kashefi, and M. Roetteler, Quadratic Form Expansions for Unitaries, *the Third Conference on the Theory of Quantum Computation, Communication and Cryptography*, Japan, TQC2008

- E. Kashefi, Lost in Translation, *the Third Workshop on Developments in Computational Models*, Poland, DCM2007

- E. Kashefi and M. Sadrzadeh, Epistemic Measurement System, *Workshop on Quantum Cryptography and Security*, Portugal, LQCIL2007

- V. Danos, E. Kashefi, and P. Panangaden, The One Way to Quantum Computation, *the 33th International Colloquium on Automata, Languages and Programming*, Italy, ICALP2006

- *V. Danos, E. D'Hondt, E. Kashefi, P. Panangaden, Distributed MBQC, *the 3rd Workshop on Quantum Programming Languages*, US, QPL2005

- *V. Danos and E. Kashefi, Pauli measurements are universal, *the 3rd Workshop on Quantum Programming Languages*, US, QPL2005

- E. Kashefi, Quantum Domain Theory - Definitions and Applications, *the International Conference on Computability and Complexity Analysis*, US, CCA2003

- *V. Vedral and E. Kashefi, Unified axiomatic approach to information content of physical states, *the 6th Conference on Quantum Communication, Measurement and Computing*, US, QCMC2002

- Edalat, A. Lieutier, and E. Kashefi, Convex hull in a new model of computation, *the 13th Canadian Conference on Computational Geometry*, Canada, CCCG2000

Articles under Consideration for Publications

- *S. Barz, V. Dunjko, F. Schlederer, M. Moore, E. Kashefi and I. Walmsley, Enhanced delegated computing using coherence, arXiv:1502.02571, Submitted to *Phys. Rev. A.*

- *J. Fitzsimosn and E. Kashefi, Unconditionally verifiable blind computation, arXiv:1203.5217, Submitted to SIAM *Journal of Computing*

Patent

- ** UK Patent Application No 1402599.3, Quantum Enhanced Secure Delegated Computing*