Curriculum Vitae

1. Personal: **Hoi-Kwong Lo**
Dept. of ECE and Dept. of Physics, 10 King's College Road, University of Toronto, Toronto ON M5S 3G4
Phone: 416-946-5525
URL: http://www.comm.utoronto.ca/~hklo
Email: hklo@comm.utoronto.ca

2. Degrees:

1989- 1994	Doctor of Philosophy (Physics) Caltech, Pasadena CA, USA Thesis Title: Exotic Phenomena in Non-Abelian Gauge Theories Thesis Advisor: Prof. John Preskill.
1989- 1991	Master of Science (Physics) Caltech, Pasadena CA. USA
1986-1989	Bachelor of Arts (Mathematics): *Triple First Class Honours.* Trinity College, Cambridge University, UK [Master of Arts (Mathematics) awarded in 1993.]

3. Employment History

2009-present	Professor and Canada Research Chair in Quantum Information, Center for Quantum Information and Quantum Control (CQIQC), Department of Physics; & Department of Electrical and Computer Engineering (ECE), University of Toronto
2009	Long-term visitor, Quantum Information Science Program, KITP, UC Santa Barbara
2002- 2009	Associate Professor and Canada Research Chair in Quantum Information, Center for Quantum Information and Quantum Control (CQIQC), Department of Physics; & Department of Electrical and Computer Engineering (ECE), University of Toronto
2006-2007	Visiting Professorship, Perimeter Institute for Theoretical Physics, Waterloo
1999-2002	Chief Scientist and Senior Vice President, R&D. MagiQ Technologies, Inc. New York, NY (www.magiqtech.com)

1997-1999	Senior Member of Technical Staff, Hewlett-Packard Labs, Bristol, UK
1996-1997	Postdoctoral Fellow, Hewlett-Packard Labs, Bristol, UK
1994-1996	Member, Institute for Advanced Study, Princeton, NJ

4. Honours and Awards

2010	Fellow of Quantum Information Science Program of the Canadian Institute for Advanced Research (CIFAR).
2008-2013	Canada Research Chair (renewal)
2007	NSERC Discovery Accelerator Supplement Award
2006-07	Visiting Professorship, Perimeter Institute for Theoretical Physics.
2005-2009	Scholar of Canadian Institute for Advanced Research (CIFAR).
2003	Co-winner, 2003 Outstanding Young Researcher Award (OYRA) by Overseas Chinese Physics Association (OCPA) (for outstanding young ethnic Chinese physicists of any place of birth and currently working anywhere outside Asia)
2003	PREA (Premier's Research Excellence Award)
2003-2008	Canada Research Chair Award
2003	Ontario Outstanding Researcher
1996	Australian Postdoctoral Research Fellowship (offered)
1996	1851 Exhibition Fellowship (to Oxford University) (offered)
1996	Hewlett-Packard Postdoctoral Research Fellowship, HP Labs, Bristol (accepted)
1986-89	Triple First Class Honors, Cambridge University
1989	Mathison Prize, Trinity College, Cambridge University The highest ranking student in applied mathematics
1988	Senior Scholar, Trinity College, Cambridge University
1987	Osborne Prize, Trinity College, Cambridge University The highest ranking student in applied mathematics
1987	Junior Scholar, Trinity College, Cambridge University
1986	Prince Philip Scholarship, Friends of Cambridge University in Hong Kong *[One of the six recipients of full-cost merit-based three-year scholarships to Cambridge University.]*

5. Professional affiliations and activities

Co-founder (with Sam Braunstein) and co-managing Editor, Quantum Information & Computation (QIC) 2001-2008

This is the leading journal in the field.
[Impact factor QIC is ranked 14th out of 1000+ IS/IT/CS/SE related journals listed in the latest (2005)ISI ranking, with

an impact factor 3.584 (PRA scores 2.997), while most journals counted by the ISI have an impact factor below 1. Other managing co-editors include luminaries David Wineland, Ignacio Cirac, Richard Jozsa, Samuel Braunstein, Bruce Kane, and Richard Cleve. Associate Editors include, for example, Ray Laflamme (Director of IQC, Waterloo) and Mike Mosca.]

Fellow of Canadian Institute for Advanced Research (CIFAR).
Senior Member of the Institute of Electrical and Electronics Engineers (IEEE)
Affiliate Member of the Perimeter Institute
Member of American Physical Society (APS)
Member of Canadian Association of Physicists (CAP)

6. **A. Research interests:** quantum information, quantum computation.

B. Research awards:

CIFAR Fellow 2010. Canada Research Chair renewed 2008-2013. NSERC Research Accelerator Supplement Award 2007. CIFAR Scholar 2005. In addition, his group has received funding from NSERC, CRC program, CFI, OIT, CIPI, MITACS and QuantumWorks.

C. Patents

1) US patent 5,732,139 ``quantum cryptographic system with reduced data loss'' (1998) by Hoi-Kwong Lo and H. F. Chau

2) European Patent EP 1,159,660 B1 ``computing apparatus and methods using secure authentication arrangement'' (2003) by Liqun Chen, Hoi-Kwong Lo and David Chan.

3) US Patent 7,197,523 B2 "Efficient Use of detectors for Random number generation", (2007) by N. Lutkenhaus, J. L. Cohen and H.-K. Lo.

Also Patent Applications

US Patent Application Number 20040141618 "Quantum Key System and Method" by H.-K. Lo and D. Gottesman.

US Patent Application Number 20040190719 "Decoupling Error Correction from Privacy Amplification in Quantum Key Distribution" by H.-K. Lo

"Method, System and Apparatus for Optical Phase Modulation Based on frequency shift", by Bing Qi, Li Qian, Hoi-Kwong Lo and Yi Zhao, US and Canadian Patent Applications (filed Dec. 1, 2006)

7. Refereed Publications

All citation counts listed below are from Google Scholar accessed on Apr. 3, 2011.

Invited Review Papers

Quantum Cryptography
H.-K. Lo and Y. Zhao,
(Invited paper) Encyclopedia of Complexity and Systems Science,Volume 8, pages 7265-7289, Springer New York, 2009

Survey Articles

S1) From Quantum Cheating to Quantum Security,
D. Gottesman and H.-K. Lo, Physics Today, Nov. 2000, p. 22.
http://www.aip.org/pt/vol-53/iss-11/p22.html
[Listed as a notable article in ``The Best American Science and Nature Writing, 2001'' edited by Ed. O. Wilson.]

S2) Cryptography's Quantum Barrier,
H.-K. Lo, Physics World, June 2000, p. 17.

Refereed Journal articles:

1) Insecurity of position-based quantum cryptography protocols against entanglement attacks, H. K. Lau and H.-K. Lo, Phys. Rev. A 83, 012322 (2011).

2) Balanced homodyne detector for high-rate Gaussian-modulated coherent-state quantum key distribution,Yue-Meng Chi, Bing Qi, Wen Zhu, Li Qian, Hoi-Kwong Lo, Sun-Hyun Youn, A. I. Lvovsky, Liang Tian, New J. Phys. 13 (2011) 013003

3) Optimal entanglement transformations among N-qubit W-class states, W. Cui, E. Chitambar, and H.-K. Lo, Phys. Rev. A 82, 062314 (2010)

4) Passive sources for the Bennett-Brassard 1984 quantum-key-distribution protocol with practical signals, M. Curty, X. Ma, H.-K. Lo, and N. Lütkenhaus, Phys. Rev. A 82, 052325 (2010).

5) Experimental demonstration of phase-remapping attack in a practical quantum key distribution system, Feihu Xu, Bing Qi, Hoi-Kwong Lo, New J. Phys. 12 (2010) 113026.

0) Feasibility of Quantum Key Distribution through a dense wavelength division multiplexing network, B. Qing, W. Zhu, L. Qian and H.-K. Lo, New J. Phys. 12 (2010) 103042.

1) Implementation of two-party protocols in the noisy-storage model

S. Wehner, M. Curty, C. Schaffner, and H.-K. Lo, Phys. Rev. A81, 052336 (2010).
http://arxiv.org/abs/0911.2302

2) Passive Estimate of an Untrusted Source for Quantum Key Distribution

Y. Zhao, B. Qi, H.-K. Lo, L. Qian, New J. Phys. 12, 023024 (2010).
http://arxiv.org/abs/0905.4225

3) High-speed quantum random number generation by measuring phase noise of a single mode laser
B. Qi, Y.-M. Chi, H.-K. Lo, L. Qian, Optics Letters 35, 312-314 (2010).
http://arxiv.org/abs/0908.3351

4)Bounds on probability of transformations between multi-partite pure states

W. Cui, W. Helwig, and H.-K. Lo, Phys. Rev. A 81, 012111 (2010).
http://arxiv.org/abs/0910.3295

5) Upper bounds for the secure key rate of decoy state quantum key distribution

M. Curty, T. Moroder, X. Ma, H.-K. Lo and N. Lutkenhaus,
Phys. Rev. A 79, 032335 (2009)
http://arxiv.org/abs/0901.4669

6) Security proof of quantum key distribution with detection efficiency mismatch
C.-H.F. Fung, K. Tamaki, B. Qi, H.-K. Lo and X. Ma,
Quantum Information and Computation 9,131(2009).
http://arxiv.org/abs/0802.3788

7) Quantum Hacking: Experimental demonstration of time-shift attack against practical quantum key distribution systems.
Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen and H.-K. Lo,
Phys. Rev. A 78, 042333 (2008)
http://arxiv.org/abs/0704.3253

8) Possibility, impossibility, and cheat sensitivity of quantum-bit string commitment
H. Buhrman, M. Christandl, P. Hayden, H.-K. Lo and S. Wehner,
Physical Review A 78, 022316 (2008).
[Selected for publication in the Virtual Journal of Quantum Information, published by the American Physical Society.]

9) Random-party entanglement distillation in multiparty states
B. Fortescue and H.-K. Lo, Phys. Rev. A 78, 012348 (2008).
http://arxiv.org/abs/0709.4059

10) Quantum key distribution with triggering parametric down conversion sources,
X. Ma and H.-K. Lo,
New J. Phys. 10, 073018 (2008)
http://arxiv.org/abs/0803.2543

11) Quantum key distribution with an unknown and untrusted source
Y. Zhao, B. Qi and H.-K. Lo,
Phys. Rev. A 77, 052327 (2008)
http://arxiv.org/abs/0802.2725

12) Quantum Cryptography: from theory to practice (Invited Paper)
H.-K. Lo and N. Lutkenhaus,
Physics in Canada, Vol. 63, no. 4, pp 191-197 (2007).
http://arxiv.org/abs/quant-ph/0702202

13) Experimental study on Gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers
B. Qi, L.-L. Huang, L. Qian and H.-K. Lo
Phys. Rev. A **76**, 052323 (2007).
http://arxiv.org/abs/0709.3666
[This paper has been selected for publication in the Dec. 10, 2007 issue of Virtual Journal of Nanoscale Science & Technology and the December 2007 issue of Virtual Journal of Quantum Information.]

14) Quantum key distribution with entangled photon sources
X. Ma, C.-H. F. Fung, and H.-K. Lo, Phys. Rev. A76, 012307 (2007).
http://arxiv.org/abs/quant-ph/0703122

15) Multi-partite quantum cryptographic protocols with noisy GHZ states
K. Chen and H.-K. Lo,
Quantum Information and Computation 7, 689 (2007),
http://xxx.lanl.gov/abs/quant-ph/0404133

16) Random bipartite entanglement from W and W-like states
B. Fortescue and H.-K. Lo, Phys. Rev. Lett. 98, 260501 (2007).

17) Quantum key distribution with "dual detectors"
B. Qi, Y. Zhao, X. Ma, H.-K. Lo and L. Qian, Phy. Rev. A 75, 052304 (2007).
http://arxiv.org/abs/quant-ph/0611044

18) Sequential attacks against differential-phase-shift quantum key distribution with weak coherent states
M. Curty, L. L.X. Zhang, H.-K. Lo and N. Lutkenhaus, Quantum Information and Computation 7, 665 (2007).
http://arxiv.org/abs/quant-ph/0609094

19) Phase-remapping attack in practical quantum key distribution systems,
C.-H. F. Fung, B. Qi, K. Tamaki, and H.-K. Lo, Phys. Rev. A **75**, 032314 (2007)
http://arxiv.org/abs/quant-ph/0601115

20) Security of quantum key distribution using weak coherent states with Nonrandom phases,
H.-K. Lo and J. Preskill, Quantum Information and Computation 7, 431 (2007).
http://arxiv.org/abs/quant-ph/0610203

21) Discrete Rotational Symmetry and Quantum Key Distribution Protocols
D. Shirokoff, C.-H. F. Fung, and H.-K. Lo, Phys. Rev. A75, 032341 (2007).
http://arxiv.org/abs/quant-ph/0604198

22) Experimental quantum key distribution with active phase randomization
Y. Zhao, B. Qi, and H.-K. Lo, Appl. Phys. Lett. **90**, 044106 (2007)
http://arxiv.org/abs/quant-ph/0611059

23) Security of quantum bit string commitment depends on the information measure
H. Buhrman, M. Christandl, P. Hayden, H.-K. Lo, S. Wehner,
Phys. Rev. Lett. **97**, 250501 (2006).
http://arxiv.org/abs/quant-ph/0504078

24) Security proof of a three-state quantum key distribution protocol without rotational symmetry
C.-H. F. Fung, and H.-K. Lo, Phys. Rev. A74, 042342 (2006)
http://arxiv.org/abs/quant-ph/0607056

25) Time-shift attack in practical quantum cryptosystems,
B. Qi, C.-H. F. Fung, H.-K. Lo and X. Ma, Quantum Information and Computation 7, 73 (2007). (10 pages)
http://arxiv.org/abs/quant-ph/0512080

26) Decoy-state quantum key distribution with two-way classical postprocessing
X. Ma, C-H. F. Fung, F. Dupuis, K. Chen, K. Tamaki, and H.-K. Lo,
Phys. Rev. A74, 032330 (2006). (16 pages)

*27) Experimental Quantum Key Distribution with Decoy States,
Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian,
Phys. Rev. Lett. 96, 070502 (2006).
http://arxiv.org/abs/quant-ph/0503192
*[This work has attracted a lot of media attention including Toronto's largest city newspaper ``Toronto Star" and MIT "Technological Reviews"
Published only three years ago, the paper has been cited by 111.]*

28) Performance of two quantum key distribution protocols,
C.-H. F. Fung, K. Tamaki and H.-K. Lo,
Phys. Rev. A73, 012337 (2006).
http://arxiv.org/abs/quant-ph/0510025

29) Quantum key distribution based on arbitrarily-weak distillable entangled states,
K. Horodecki, D. Leung, H.-K. Lo, and J. Oppenheim,
Phys. Rev. Lett. 96, 070501 (2006).
http://arxiv.org/abs/quant-ph/0510067

30) Unconditionally secure key distillation from multiphotons
K. Tamaki, and H.-K. Lo,
Phys. Rev. A73, 010302(R) 2006
http://arxiv.org/abs/quant-ph/0412035

31) Two-way quantum communication channels,
A. Childs, D. W. Leung, and H.-K. Lo,
International Journal of Quantum Information 4, No. 1, (Asher Peres Memorial Issue) pp. 63-83 (2006)
http://arxiv.org/abs/quant-ph/0506039

32) Frequency-shifted Mach-Zehnder Interferometer for Locating Multiple Weak Reflections along a Fiber Link,
B. Qi, L. Qian, A Tausz, and H.-K. Lo,
IEEE Photonics Technology Letters 18, 295 (2005).

33) High-resolution, large dynamic range fiber length measurement based on a frequency-shifted asymmetrical Sagnac interferometer,
B. Qi, A. Tausz, L. Qian, and H.-K. Lo,
Optics Letters 30, No. 24, 3287 (2005).

34) Practical decoy state for quantum key distribution,
X. Ma, B. Qi, Y. Zhao, and H.-K. Lo,
Phys. Rev. A72, 012326 (2005).
http://arxiv.org/abs/quant-ph/0503005

*35) Decoy State Quantum Key Distribution,
H.-K. Lo, X. Ma, and K. Chen,
Phys. Rev. Lett. 94, 230504 (2005).
http://arxiv.org/abs/quant-ph/0411004
[This work has been highlighted in international popular and scientific press including the largest Canadian newspaper "Globe and Mail" and "New Scientist". Published four years ago, the paper has been cited by 286.]

36) Inefficiency and classical communication bounds for conversion between partially entangled pure bipartite states,
B. Fortescue and H.-K. Lo,
Phys. Rev. A **72**, 032336 (2005).
http://xxx.lanl.gov/abs/quant-ph/0411200

37) Getting something out of nothing,
H-K. Lo,
Quantum Information and Computation Vol 5, No. 4&5 (2005) 413-418.
http://arxiv.org/abs/quant-ph/0503004

38) Efficient Quantum Key Distribution Scheme and Proof of its Security,
H.-K. Lo, H. F. Chau, M. Ardehali,
J. of Cryptology, 18, Number 2, (2005) 133-165.
http://arxiv.org/abs/quant-ph/0011056.

39) Some attacks on quantum-based cryptographic protocols
H.-K. Lo and T.-M. Ko,
Quantum Information and Computation. Vol. 5, No.1 (2005) 40-47.
http://xxx.lanl.gov/abs/quant-ph/0309127

40) Security of quantum key distribution with imperfect Devices,
D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill,
Quantum Information and Computation. Vol. 4, No.5 (2004) 325-360.
http://xxx.lanl.gov/abs/quant-ph/0212066
[Cited by 243.]

41) A Tight Lower Bound on the Classical Communication Cost of Entanglement Dilution,
A. Harrow and H.-K. Lo,
IEEE Transactions on Information Theory,
Vol. 50, Issue 2, pp. 319-327 (2004)
http://xxx.lanl.gov/abs/quant-ph/0204096

42) Method for decoupling error correction from privacy amplification,
H.-K. Lo, New Journal of Physics 5, 36 (2003). (Invited paper)
http://xxx.lanl.gov/abs/quant-ph/0201030

43) Proof of Security of quantum key distribution with two-way

classical communications,
D. Gottesman and H.-K. Lo,
IEEE Transactions on Information Theory, Vol. 49, No. 2,
p. 457 (2003).
http://xxx.lanl.gov/abs/quant-ph/0105121
[Cited by 136.]

44) Proof of Unconditional Security of Six-State Quantum Key Distribution Scheme,
H.-K. Lo, Quantum Information and Computation, Vol. 1, Number 2, 81 (2001).
http://xxx.lanl.gov/abs/quant-ph/0102138

45) A Simple Proof of the Unconditional Security of Quantum Key Distribution,
H.-K. Lo, J. of Phys. A, Vol. 34, 6957 (2001).
http://xxx.lanl.gov/abs/quant-ph/9904091

*46) Concentrating Entanglement by Local Actions: Beyond Mean Properties,
H.-K. Lo and S. Popescu, Phys. Rev. A, Vol. 63, 022301 (2001).
http://xxx.lanl.gov/abs/quant-ph/9707038

47) A Quantum Analog of Huffman Coding,
S. L. Braunstein, C. A. Fuchs, D.Gottesman, and H.-K. Lo, IEEE Transactions on Information Theory, Vol. 46, 1644 (2000).
http://xxx.lanl.gov/abs/quant-ph/9805080

48) Classical-communication cost in distributed quantum-information processing: a generalization of quantum-communication complexity,
H.-K. Lo, Phys. Rev. A, Vol. 62, 012313 (2000).

*49) Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances,
H.-K. Lo and H. F. Chau, Science Vol. 283, 2050 (1999).
http://xxx.lanl.gov/abs/quant-ph/9803006
[Cited by 595. Highlighted by a Perspective article in Science by Peter Shor and Charles Bennett.]

*50) How to Share a Quantum Secret,
R. Cleve, D. Gottesman and H.-K. Lo,
Physical Review Letters Vol. 83, 648 (1999).
http://xxx.lanl.gov/abs/quant-ph/9901025

51) Classical Communication Cost of Entanglement Manipulation:
Is Entanglement an Interconvertible Resource?,
H.-K. Lo and S. Popescu, Physical Review Letters, Vol. 83, 1459 (1999).
http://xxx.lanl.gov/abs/quant-ph/9902045

52) Making An Empty Promise With A Quantum Computer, (Invited Paper)
H. F. Chau and H.-K. Lo, Fort. de. Phys., Vol. 46, No. 4-5, 325 (1998).
http://xxx.lanl.gov/abs/quant-ph/9709053
[Also, re-published in the book ``Quantum Computing'', eds. S. Braunstein.
http://www.sees.bangor.ac.uk/~schmuel/book/book1.html]

53) Why Quantum Bit Commitment and Ideal Quantum Coin Tossing
Are Impossible,
H.-K. Lo and H. F. Chau, Physica D, Vol. 120, 177 (1998).
http://xxx.lanl.gov/abs/quant-ph/9711065

54) Insecurity of Quantum Secure Computations,
H.-K. Lo, Phys. Rev. A, Vol.56, 1154 (1997).
http://xxx.lanl.gov/abs/quant-ph/9611031

*55) Is Quantum Bit Commitment Really Possible?
H.-K. Lo and H. F. Chau, Phys. Rev. Lett., Vol. 78, 3410 (1997).
http://xxx.lanl.gov/abs/quant-ph/9603004
[This fundamental result has been highlighted in Science and Science News.]

56) One Way Functions in Reversible Computations,
H. F. Chau and H.-K. Lo, Cryptologia, Vol. 21, No. 2, 139 (1997).
http://xxx.lanl.gov/abs/quant-ph/9506012

57) Primality Test via Quantum Factorization,
H. F. Chau and H.-K. Lo, International Journal of Modern Physics C,
Vol. 8, No. 2, 131 (1997).
http://xxx.lanl.gov/abs/quant-ph/9508005

58) Quantum coding Theorem for mixed states,
H.-K. Lo, Optics Communications, Vol. 119, 552 (1995).
http://xxx.lanl.gov/abs/quant-ph/9504004

59) Aharonov-Bohm Order Parameters for Non-Abelian Gauge Theories,
H.-K. Lo, Phys. Rev. D, Vol. 52, 7247 (1995).
http://xxx.lanl.gov/abs/hep-th/9502080

60) Is Baryon Number Violated when Electroweak Strings Intercommute?
H.-K. Lo, Phys. Rev. D, Vol. 51, 7152 (1995).
http://xxx.lanl.gov/abs/hep-ph/9409319

61) Scattering from Electroweak Strings,
H.-K. Lo, Phys. Rev. D, Vol. 51, 802 (1995).
http://xxx.lanl.gov/abs/hep-ph/9404273

62) Exact Wave Functions for non-Abelian Chern-Simons Particles,
H.-K. Lo, Phys. Rev. D, Vol. 48, 4999 (1993).

http://xxx.lanl.gov/abs/hep-th/9306076

63) Complementarity in Wormhole Chromodynamics,
H.-K. Lo, K.-M. Lee and J. Preskill, Phys. Lett. B, Vol. 318, 287 (1993).
http://xxx.lanl.gov/abs/hep-th/9308044

64) Non-Abelian Vortices and non-Abelian Statistics,
H.-K. Lo and J. Preskill, Phys. Rev. D, Vol. 48, 4821 (1993).
http://xxx.lanl.gov/abs/hep-th/9306006

65) Topological Approach to Alice Electrodynamics,
M. Bucher, H.-K. Lo and J. Preskill, Nucl. Phys. B, Vol. 386, 3 (1992).
http://xxx.lanl.gov/abs/hep-th/9112039

Preprints

P1) arXiv:1011.2982 [pdf, ps, other]
Title: Universal Squash Model For Optical Communications Using Linear Optics And Threshold Detectors
Authors: Chi-Hang Fred Fung, H. F. Chau, Hoi-Kwong Lo
Comments: 14 pages
Subjects: Quantum Physics (quant-ph)

P2) arXiv:1005.0272 [pdf, other]

Title: Security of high speed quantum key distribution with finite detector dead time

Authors: Viacheslav Burenkov, Bing Qi, Ben Fortescue, Hoi-Kwong Lo

Comments: 18 pages, 7 figures

P3). A brief introduction of quantum cryptography for engineers
B. Qi, L. Qian and H.-K. Lo
http://arxiv.org/abs/1002.1237

Publications by group members
[Group members are encouraged to publish their results on their own.]

G1) Unconditional security at a low cost

by Xiongfeng Ma, Phys. Rev. A. 052325 (2006).

G2) Bing Qi, Li Qian, "Optimal filters for photon cloning with an optical amplifier", Optics Letters **32**, 418-420 (2007).

G3) Bing Qi, "Single photon continuous variable quantum key distribution based on energy-time uncertainty relation," Optics letters 31, 2795-2797 (2006) (This paper has been selected for publication in the September 11, 2006 issue of Virtual Journal of Nanoscale Science & Technology and the September 2006 issue of Virtual Journal of Quantum Information)

G4) Marcos Curty, Xiongfeng Ma, Bing Qi, Tobias Moroder, "Passive decoy state quantum key distribution with practical light sources", Physical Review A 81, 022310 (2010)

G5) Fei Ye, Li Qian, and Bing Qi, "Multipoint Chemical Gas Sensing Using Frequency-Shifted Interferometry", Journal of Lightwave Technology 27, 5356-5364 (2009)

B. Books

Book chapter: Quantum cryptology, Chapter 4 of Introduction to quantum computation and information, eds. H.-K. Lo, S. Popescu, and T. Spiller (World Scientific, Singapore, Hardcover 1998, Paperback 2000).
http://www.worldscientific.com/books/physics/3724.html

C. Books edited

1) Introduction to quantum computation and information,
eds. H.-K. Lo, S. Popescu, and T. Spiller (World Scientific, Singapore, Hardcover 1998 Paperback 2000).
http://www.worldscientific.com/books/physics/3724.html
[Cited by 211. Reviewed in Nature 339, p. 119 (1999).]

2) As an editor: Scalable quantum computers: paving the way to realization,
eds. S. L. Braunstein and H.-K. Lo (Wiley-VCH, Berlin, 2000).
http://www.sees.bangor.ac.uk/~schmuel/book/book2.html

8. Selected Invited Talks

Over 45 invited talks over the last seven years. Some examples are:

2nd Workshop on Quantum Information Science, Hong Kong Poly. U., Jan. 2011.
CIFAR Quantum Information Processing Meeting, Toronto, Nov. 2010.
Physics Colloquium, University of Hong Kong, March 2010
Physics Seminar, Hong Kong University of Science and Technology, Feb. 2010.
Quantum Information Science Program, KITP, UCSB, October 09
Classical and Quantum Information Assurance Foundations and Practice, Dagstuhl Workshop, July 09

Topical Team Meeting, Space-QUEST project, Austria, October 08
European SECOQC QKD public demonstration, Austria, October 08
QCMC (Quantum Communication, Measurement and Computing) 08, Calgary, August 08
Information Security in a Quantum World, IQC, Waterloo, August 08.
CEQIP'08 (5 th Central European Quantum Information Processing Workshop) Czech Republic, June 2008
University of Hong Kong, Physics Dept.,May 2008.
Chinese University of Hong Kong, Physics Department Seminar, Jan. 2008.
Brock University, Physics Departmental Seminar, Oct. 2007.
Lisbon Workshop on Quantum Cryptography and Security. July 2007
Invited speaker, American Physical Society March Meeting (declined for personal reason), March 2007.
University of Hong Kong, Physics Dept., March 2007.
University of Buffalo, Physics Seminar, Oct. 2006
Fields Institute "Quantum Cryptography and Computing Workshop", Oct., 2006.
Perimeter Institute, Invited Talk, Sept. 2006.
International Conference on Quantum Foundation and Technology: Frontier and Future, Hangzhou, China, August 2006.
Gordon Research Conference, Italy, Discussion Leader, May 2006.
Certicom, Lunch and Learn, March 2006.
Caltech Workshop "Classical and Quantum Security", Dec. 2005.
University of Erlangen-Nuremberg, July 2005
Benasque Workshop on Quantum Information, June-July 2005.
CIAR meeting, Halifax, May 2005.
IQI Seminar, Caltech, March 2005.
First Asia-Pacific Conference on QIS, Taiwan, Dec. 2004
Special Week on Quantum Cryptography, Isaac Newton Institute, Sept. 2004.
QIT: Present Status and Future Directions, Isaac Newton Institute, Sept. 2004.
Conference on Quantum Information and Quantum Control, Fields Institute, Toronto, July 2004.
Eastern Formosa Summer School, June, 2004
Workshop on Quantum Information, Tainan, Taiwan, June, 2004.
Colloquium, Academic Sinica, Taiwan, June 2004.
RSA Japan Conference, May-June, 2004.
Fields Institute Workshop on Quantum Geometry and Q. Computing, May 2004.
Invited talk at National Research Council, Ottawa, May 2004
Physics Division Colloquium, Los Alamos National Labs, April 2004.
Invited talk at U. of Michigan, April 2004.
Snowmass Conference on Quantum Electronics, Utah, Jan. 2004.
Invited talk, CIAR Quantum Information Processing Program, Oct. 2003.
Invited talk at, Center for Photonic Communications and Computing, Northwestern University, Oct. 2003.
Photonics North, Montreal, May 2003,
http://www.hospitalite.com/pn2003/pn_welcome.html

Workshop on "Cryptographic Reduction in Classical and Quantum Cryptography", Montreal, May 2003.
James H. Simons Conference, Stony Brook, New York, USA, May 2003
Invited talk at ACM Toronto Chapter, March 2003.
Workshop on Quantum Information, Cryptography and Error Correction MSRI, Berkeley, Nov. 2002
Physics Society Japan (JPS) Autumn Meeting, Nagoya, Japan, Sept. 2002.
EQIS' 02 (ERATO Quantum Information Science), Tokyo, Japan, Sept. 2002.
Feynman Festival, College Park, M.D., August 2002.
Quantum Communications, Measurements and Computing (QCM&C) 2002, Boston, July 2002.
Quantum Device Technology workshop, Clarkson University, May 2002
RSA Conference 2002, San Jose, CA, Feb. 2002
EuroWorkshop on ``Quantum Computing Theory''. Torino, Italy, June, 2001.
Quantum Communications, Measurements and Computing (QCM&C) 2000, Capri, Italy, June, 2000
Instructional Course in Quantum Computing, Edinburgh, UK, March 2000.
Quantum Information Processing 2000 Workshop, Montreal, CA, Dec. 1999
Princeton workshop on ``quantum cryptography", Princeton, NJ, Nov., 1999
Issac Newton Institute workshop on ``Physics of Information'', Cambridge, UK, June 1999.
Dagstuhl seminars on quantum computation, Dagstuhl, Germany, 1998.

Contributed Conference Talks delivered by Lo' group

In addition, Lo's group members have delivered over 30 Contributed conference talks and other invited talks in the last seven years. These include 10 Talks at IEEE ISIT (International Symposium on Information Theory), which is the top conference in information theory. 6 Talks at the AQIS conference, which is the top Asian Pacific Conference on Quantum Information, and invited talks at places such as the Perimeter Institute for Theoretical Physics, Waterloo and the Institute for Quantum Information (IQC), Waterloo, and Caltech.

9. Courses Taught

A. Undergraduates		Enrollment
2003 Fall	PHY256F Introduction to Quantum Physics	87
2004 Fall	ECE310F Linear systems and communications	60
2005 Spring	PHY281S Elements of Physics III (Quantum Physics)	174
2006 Spring	PHY281S Elements of Physics III (Quantum Physics)	195
2006 Spring	ECE216S Signals and Systems	77
2007 Full	ECE496 Design Project (Lo is one of the course Administrators)	38

2008 Full	ECE496 Design Project (Lo is one of the course Administrators)	35
2011 Spring	APS112 Engineering Strategies and Practices II	~100

*In 2006 Spring Semester, Lo was the coordinator of the course PHY281.

B. Graduates		Enrollment
2003 Fall	ECE1531F Quantum Information Theory	9
2004 Fall	ECE1531F Quantum Information Theory	9
2005 Fall	ECE1531F Quantum Information Theory	8
2007 Fall	PHY2211/ Quantum Information Theory ECE1531	13
2007 Fall	PHY1520F Quantum Mechanics	12
2008 Fall	PHY2211/ Quantum Information Theory ECE1531	12
2008 Fall	PHY1520F Quantum Mechanics	23
2009 Fall	PHY2211/Quantum Information Theory ECE1531	
2009 Fall	PHY1520F Quantum Mechanics	
2011 Fall	PHY2211/Quantum Information Theory ECE1531	
2011 Fall	PHY1520F Quantum Mechanics	

*Designing a New Course: ECE1531F Quantum Information Theory is a new course designed solely by Lo. It is an interdisciplinary course taken by physicists and engineers alike. This is the only course in quantum information that is being offered by the University of Toronto.

*Obtained Certificate on "Mastering the Craft of University Teaching" from the Office of Teaching Advancement at the University of Toronto (2005).

C. Training of highly qualified personnel

Training of highly qualified persons is an important part of Lo's research program. He attracted top students from top universities such as Oxford University, Imperial College London, Peking University and the University of Toronto. Those trainees' have figured prominently in the achievements of the group. His postdocs and students have won a number of honours/recognition. For instance, his former postdoc, Dr. Kai Chen has won an Alexander von Humboldt Foundation Fellowship in Germany. Four of his current and former group members (J. C. Boileau, F. Dupuis, F. Fung, and Y. Zhao) have won NSERC postdoctoral fellowships. Furthermore, three of his former group members have already secured long-term positions. Dr. Kiyoshi Tamaki is currently a permanent

research staff member at NTT, the largest telecom firm in Japan, Dr. Marcos Curty is an Associate Professor at the University of Vigo, (his hometown) in Spain and Dr kai Chen is a Full Professor at the University of Science and Technology of China.

Ph.D students supervised and theses completed
(2009) Yi Zhao, Quantum Cryptography in Real-life Applications
(2009) Benjamin Fortescue, Application and Manipulation of bipartite and multipartite entangled quantum states
(2008) Xiongfeng Ma, Quantum Cryptography, from theory to practice
(2008) Chi-Hang Fred Fung, Security and Performance Analysis of Quantum-Key-Distribution Systems

Master students supervised or co-supervised
(2009) Yuemeng Chi
(2009) Cathal Smyth
(2008) Viacheslav Burenkov
(2008) Gigi Wong
(2008) Ayman Shalaby
(2006) Leilei Huang
(2005) Jamin Sheriff
(2005) Yi Zhao
(2004) Benjamin Fortescue
(2004) Xiongfeng Ma
(2003) Mohammed Abdelghani

D. Other teaching and lectures given

Design Project Supervision

In 2004-05, he supervised a design project for three students (Jimmy Truong Jonathan Sy, Matthew Hum) to build an educational demo for information reconciliation.

10. Administrative Positions

A. University and Department Committee
- Founding Member and Management Committee Member (2004-2011), Center for Quantum Information and Quantum Control (CQIQC)
- Advisory Committee Member, Institute for Applied and Interdisciplinary Mathematics.
- Admission Committee, Physics Dept. (2007-2008)
- Faculty Search Committee on the area of Information Security, ECE Dept. (2007-2008)

- Communications and Publicity Committee, Physics Dept.(2004-2006)
- Standards and Evaluations Committee, Physics Dept.(2004-2006)
- Faculty Search, Senior Quantum Optics Position. [Initial Phase only.] (2004-2005)

B. Scholarly and Professional

Co-founder with Sam Braunstein and Founding Managing Editor of Quantum Information & Computation (QIC) 2001-2008
This is a leading journal in the field.
[Impact factor QIC is ranked 14th out of 1000+ IS/IT/CS/SE related journals listed in the latest (2005)ISI ranking, with an impact factor 3.584 (PRA scores 2.997), while most journals counted by the ISI have an impact factor below 1. Other managing co-editors include luminaries David Wineland, Ignacio Cirac, Richard Jozsa, Samuel Braunstein, Bruce Kane, and Richard Cleve. Associate Editors include, for example, Ray Laflamme (Director of IQC, Waterloo) and Mike Mosca.]

NSERC Grant Selection Committee Member 2005-06
(331) Computing and Information Sciences-B

A Nominator of Nobel Prize in Physics 2009

Nominator of Kyoto Prize in Basic Sciences 2006, 2010
[Prize money of over US$400,000 per prize.]

Referee for Kilam Fellowships and Steacie Fellowships
(Highly competitive awards for senior researchers and rising stars Respectively).

Referee for the NSERC Herzberg Medal, the Council's highest honour with $1 million Prize value.

Participation in European QKD standardization effort as a member of the Specialists Task Force (STF 367 (ISG/QKD)) of ETSI 2008-present

Topical Team Member of Space-QUEST, a European proposal For space QKD and entanglement research 2008-present

Member of the Advisory and Award Committee of the conference series "Quantum Communications, Measurements and Computation" QCM&C, which is a key conference in quantum information. We helped selected the winners of a prestigious prize in quantum communications and measurements. 2000, 2002
http://rleweb.mit.edu/qcmc/

Technical Program Committee Member of IEEE ISIT 2006
(International Symposium on Information Theory) 2006.
[This is the most important information theory conference.]

Co-organizer of CQIQC-Fields conferences 2004, 2006, 2009

Program Co-Chair of AQIS 06, a natural continuation of the 2006
[EQIS conference series, the most important Asia-Pacific conference in quantum information.]

Program Committee of AQIS 07, AQIS08, AQIS 09 2007, 2008, 2009

Program Committee of EQIS' 03, EQIS' 04, EQIS'05, 2003-2005
[http://www.qci.jst.go.jp/eqis04/ ,which is the main Asia-Pacific conference in quantum information.]

Program co-chair for the conference series 2002 and 2004
"Quantum Optics in Computing and Communication"
organized by SPIE and Chinese Optical Society.

Program Committee Member of the workshop "Theory 2008, 2010
and Realization Of Practical Quantum Key Distribution", Waterloo,

Program Committee Member of TQC(Workshop on Theory of Quantum Computation, Communication and Cryptography), 2008, 2010, 2011

Program Committee Member of QELS 2: Single and Entangled Photons and Quantum Information in CLEO/QELS'08 Conference, May 2008.

Co-organizer of Dagstuhl Workshop "Classical and Quantum Information Assurance Foundations and Practice", July 09.

Guest Editor (with Sam Braunstein), Special Issue, Fort. De. Phys. 1998

Special Issue co-Editor, Quantum Information and Computation. 2002, 2005

Co-editors of SPIE's Proceedings on "Quantum Optics in 2002 and 2004
Computing and Communication".

Consulting Scientist and International Advisory Board Member, 2003-2005
MagiQ Technologies, Inc.

Industrial Advisor to EQCSPOT (European Quantum 1998
Cryptography and Single Photon Optical Technologies) Project
https://www.cordis.lu/esprit/src/28139.html

Official Collaborator of DURINT proposal on "Novel Approaches to Quantum Computation Using Solid-State qubits" by SUNY, Stony Brook (including Dima Averin and James Lukins), University of Kansas, TRW, NIST and MagiQ. 2001

Principal Investigator (with Richard Jozsa, Sandu Popescu, and Tim Spiller) of a research proposal approved for funding by the US Army Research Office in 1998, for two postdocs over three years. This was the only proposal in quantum information processing submitted outside the US that was accepted for funding. Hewlett-Packard finally declined to receive the funding for internal reasons. 1998

Co-investigator of Hong Kong Government RGC Research Grant, HKU 7095/97F (with HF Chau of University of Hong Kong) 1997-99

Member of scientific proposal "Quantum Information Theory and Quantum Computation" funded by European Science Foundation co-ordinated by Dr. Martin Plenio. 1999

Member of UK Quantum Computing Network, co-ordinated by Prof. Richard Jozsa. 1999

Member of UK Quantum Optics Network, co-ordinated by Prof. Peter Knight. 1999

Referee for top journals in Physics, Electrical Engineering, Mathematics and Computer Science including:

i) Nature
ii) Physical Reviews Letters
iii) Physical Review A
iv) IEEE Transactions on Information Theory
v) IEEE Transactions on Computers
vi) Journal of Computer and System Sciences (full papers for STOC)
vii) Journal of Cryptology

Reviewer for *Mathematical Reviews*, a publication of the American Mathematical Society.

Refereed a number of NSERC Discovery, CFI, Canada Research Chair applications.

Reviewer for US NSF Career Awards. Invited to join a NSF review panel.

Reviewer for proposals in Hong Kong Research Grant Committee (RGC).

NSERC grant selection committee member. See above.

Nominator of Kyoto Prize of prize value about US$400,000 per prize. See above.

External Referee for tenure review cases in two top ten EE/CS departments in the US.

External Referee for the establishment of the Cambridge University-MIT quantum information collaboration.
http://cam.qubit.org/research_grants/CMI/aims.php

Referee for top conferences including Foundations of Computer Science (FOCS) and STOC (Symposium on Theory of Computing) 2008.