

MITACS Quantum Information Processing Project

Detailed scientific description of research areas and future goals

1 Quantum algorithms and complexity theory

We have made significant progress in four areas: the development of new quantum algorithms; the development of new techniques for lower bounding the computational difficulty of problems; the theory of quantum communication complexity; and the theory of quantum interactive proof systems.

1.1 Quantum algorithms

With respect to algorithms, we have designed an optimal quantum query algorithm for element distinctness [11], the problem of finding two equal elements in a collection of n elements. The algorithm uses quantum walks (quantum analogues of random walks) to perform a quantum search in a novel way. This yields an improvement over previous quantum search algorithms. Our approach has subsequently been used by Magniez, Santha and Szegedy to design a quantum algorithm for finding cliques in graphs and by Burhman and Spalek to design quantum algorithm for verifying matrix identities.

Using similar methods [13] we designed a quantum algorithm for the spatial search problem of finding a marked item among n items on a $\sqrt{n} \times \sqrt{n}$ grid.

We have also studied the problem of testing the commutativity of a black-box group given by its generators. The classical complexity of this problem was first considered by Pak in 2000. The straightforward algorithm for the problem has complexity $O(k^2)$, where k is the number of generators, since it suffices to check if every pair of generators commute. Pak presented a surprising randomized algorithm whose complexity is linear in k , and also showed that the deterministic lower bound is quadratic. The linear upper bound on complexity may also be obtained by applying Grover's algorithm to locate a pair of generators that do not commute. Using a quantization of random walks discovered by Szegedy in 2004, we obtained a *sublinear* algorithm with time and query complexity in $\tilde{O}(k^{2/3})$ (where the \tilde{O} notation means that logarithmic multiplicative factors are omitted). This appears to be the

first natural problem for which a quantum walk framework due to Szegedy has no equivalent using other known techniques for constructing quantum algorithms, such as Grover search, or the type of quantum walk introduced in [11]. (Conversely, for Triangle Finding, the approach of [11] was more successfully applied. For this problem, Magniez, Szegedy and Santha construct a quantum algorithm that uses recursively two quantum walks *a la* [11], while the Szegedy quantization of walks seems to give a less query-efficient algorithm. The problems of group commutativity and triangle finding thus give strong evidence that the walks of [11] are not comparable to the ones of Szegedy.

We have also obtained [6] a new quantum algorithm for simulating the evolution of sparse Hamiltonians (whose non-zero entries are given as a black box that computes them in adjacency-list form). One application of this is an efficiency improvement in the simulation of continuous-time quantum walk model that was introduced by Farhi and Guttmann.

Amplitude amplification, one of the main techniques in quantum algorithms, is based on the choice of certain complex numbers. In [105], we discuss the influence of the choice of these numbers on the performance of the technique. We have a partial understanding of the significance of these phases on quantum algorithms based on amplitude amplification. It is interesting to investigate how these new findings are related to error-correction and other models in which errors occur, and to widen the use of amplitude amplification.

Finally, in [145], we have shown how to make the quantum Fourier transform exact (with consequences including making the discrete logarithm algorithm exact).

1.2 Lower bounds

We have developed two new versions of the so-called quantum adversary method. We have used the first of them, the weighted adversary method [9], to solve an open problem about the relation between quantum query complexity and the polynomial degree. It was well known that the polynomial degree is a lower bound for quantum query complexity but it was open whether this bound is optimal. We solved this problem by constructing an example in which quantum query complexity is higher than the polynomial degree. We have used the second of them to prove lower bounds for simultaneously solving many instances of quantum search. These bounds are known as direct product theorems and are useful for studying the space complexity of quantum algorithms.

In [108, 106], we discuss known techniques for proving lower bounds for quantum query complexities. One main research goal is to extend these methods to new classes of partial functions, an area in which we only have a few good lower bounds.

1.3 Communication complexity

We have explored the communication costs of problems with restricted communication structures. In some scenarios there are ways of conveying information with many fewer, even exponentially fewer, qubits than possible classically. Moreover, some of these methods have a very simple structure—they involve only a few message exchanges between the communicating

parties. It is therefore natural to ask whether *every* classical protocol may be transformed to a “simpler” quantum protocol—one that has similar efficiency, but uses fewer message exchanges.

In previous work, we showed that for any constant k , there is a problem such that its $k+1$ message classical communication complexity is exponentially smaller than its k message quantum communication complexity. This, in particular, proves a round hierarchy theorem for quantum communication complexity, and implies, via a simple reduction, an $\Omega(n^{1/k})$ lower bound for k message quantum protocols for Set Disjointness for constant k .

Continuing in this direction, we prove information-theoretic lemmas, and define a related measure of *correlation*, the *informational distance*, that we believe may be of significance in other contexts as well. We improve the lower bound on the tree version of pointer jumping from $\Omega(n/k^4)$ to $\Omega(n/k)$. For the pointer jumping function itself, we improve the bound from $\Omega(n/2^{2^k})$ to $\Omega(n/2^k)$. One of the main tools, the *Average encoding lemma* based on quantum Hellinger distance, has also led to stronger relations between the communication and the number of rounds required for Set-Disjointness (Jain *et al*). Other applications of our methods include lower bounds for data structures in the well-studied cell probe model, and privacy in communication.

We have made progress in the study of properties of “non-local” effects in quantum mechanics, where local realism is violated. We sometimes refer to such effects as “pseudo-telepathy”—when, in a multi-party setting, classical players need to communicate to perfectly perform some task whereas quantum player can achieve success with certainty without any communication. We have made several contributions to this field. For example, we show that pseudo-telepathy is not possible for two players if they do not share at least an entangled pair of three-dimensional systems [37]. We also recast a scheme previously proposed by Mermin into a more “information processing language” [36].

1.4 Quantum interactive proof systems

Within the past two years, we have made significant progress in our understanding of quantum interactive proof systems. This progress is represented in the papers [150, 81, 144, 82, 51] listed in the publications section.

The paper [150] proves that a fairly natural computational problem is complete for the class QIP, which comprises those problems having quantum interactive proof systems. This computational problem is essentially to determine whether two given quantum mechanical processes are effectively the same or are different. This is an interesting fact because it gives an alternate characterization of QIP that makes no reference to quantum interactive proofs, providing further evidence that this is an interesting and natural complexity class. We hope that this may also help to prove further results concerning QIP (for instance the closure of QIP under complementation, or possibly the equality QIP=PSPACE).

The papers [81, 82] investigate the expressive power of quantum interactive proof systems with two competing provers. In addition to establishing various relations among complexity classes defined by quantum interactive proofs, this work led us to an interesting and funda-

mental problem in quantum information, and to a solution to this problem. The problem was to establish a relationship between the minimal trace distance between two given convex sets of quantum states and the probability with which one can distinguish states drawn from such sets. The relationship generalizes, in essentially an ideal way, a well-known relationship that holds for the special case where each set consists of a single state.

Finally, the paper [144] proves various facts about quantum Arthur-Merlin games, which are restricted forms of quantum interactive proofs. One of the main results is a method for error reduction in so-called QMA protocols which avoids any increase in the number of qubits that are communicated. This has interesting applications concerning the class QMA.

1.5 Future goals

There are still many unanswered questions about quantum interactive proof systems that we plan to investigate. One of our main goals is to understand the power of multi-prover interactive proof systems. Our work in [51] represents some progress in this direction, but is primarily concerned with very restricted types of multi-prover quantum interactive proofs – very little is known about the general case. Another goal is to understand the implications of quantum information to zero-knowledge interactive proof systems. This issue has thus far represented a difficult problem in theoretical quantum cryptography.

We will continue the work on quantum walks, in several directions. First, the element distinctness algorithm is a quite natural subroutine for constructing new quantum algorithms. We will look at applying it to other problems. Second, we plan to study the mixing times of quantum walks. Classically, several well-known polynomial time randomized approximation algorithms (for example, the recent approximation algorithm for permanent or algorithms for volume estimation) have been based on mixing times of Markov chains. We will investigate the possibility of using quantum walks instead of Markov chains.

We will continue the work on the new variants of quantum adversary method. There is a variety of problems for which new methods might be useful. Improving the best known lower bound for AND-OR trees has been a longstanding open problem. The complexity of several graph problems (such as finding a triangle, a clique or a perfect matching) is open and both better algorithms and better lower bounds may be possible.

A very interesting and recent model for quantum computing is a model based only on measurements. The model does not allow for unitary operations, only measurements. It is known to be universal, but most computational aspects of the model are still unknown. A research goal is to investigate these and find computational problems that are well-suited to the model. We are interested in addressing what resources are required for efficient quantum computations if only measurements are allowed, and find explicit problems that can be computed efficiently in this model.

We are currently investigating the possibility that the class PSPACE is contained in the class QIP(2) (two-message quantum interactive proof systems). We have made some progress on information theoretically secure two-prover bit commitment. We are now investigating the implication of our result on oblivious transfer. We are also studying the power of entan-

glement under the assumption that P is different from NP—we might be able to show some lower bound on entanglement in a symmetric state under those assumptions.

2 Quantum communication and information security

We have made significant progress in three areas: some new multi-party cryptographic protocols that employ quantum information; new variants of quantum key distribution protocols; and results about the cryptographic consequences of measure concentration.

2.1 Multiparty quantum communication protocols

Recently, a number of important results have shaken the world of two-party cryptographic protocols in quantum computing scenario. After many years of negative results related to Mayers, and Lo and Chau’s no-go theorem for quantum bit commitment, it is now conceivable that two-party protocols may be accomplished securely in a specific scenario. In particular, we recently showed [53] that in a scenario where two provers are involved it is possible to construct a secure bit commitment even when quantum adversaries are involved. The only drawback of this construction is that provers must be physically unable to communicate during the protocol takes place, and moreover they must never again be allowed to communicate if they are proven to cheat the protocol. However, we have presented scenarios where interesting goals may be accomplished under the assumptions outlined above.

While it is well-known that quantum bit commitment is impossible, we have studied the possibilities for a weaker primitive known as quantum string commitment in [42]. The goal is to allow one party (Alice) to “commit” to a secret string in such away the other party (Bob) cannot learn the string until Alice agrees to reveal it. We show that this is essentially impossible under the strongest definitions of security but could be achieved if a weaker but still fairly robust criterion is used.

We have also generalized hiding of quantum information to the multiparty scenario. We considered the task to distribute a state among n parties such that they all contribute to the eventual recovery of the quantum data, but only some are physically together to do so. We showed that if the largest group of get-together has at least k shares, they can decode for the quantum state, but below that threshold value, the n parties cannot learnt much about the hidden quantum state. This supplements results in quantum threshold secret sharing in the LOCC setting.

2.2 Key distribution protocols

We have investigated a method is to use “decoy states” [137] to detect eavesdropping attacks in quantum key distribution protocols. This permits a notion of unconditional security (guaranteed by the fundamental laws of physics) and yet dramatically surpasses many experimental real-world performances reported in the recent literature.

We also established results concerning the composability of quantum key distribution schemes [22], showing that they are secure enough to be used along with any other application provided an appropriate security criteria is chosen and be satisfied.

2.3 Cryptographic consequences of measure concentration

The one-time pad is perhaps the simplest and most basic cryptographic construction: two parties can use a number of secret shared random bits as key to securely encrypt and decrypt a message of the same length. An analogous construction exists in the quantum realm, with the twist that the number of bits of key required to perfectly encrypt the message is now twice the length of the message itself. Using a randomized construction exploiting measure concentration in high dimensions, we showed that this extra factor of two disappears entirely if tiny deviations from perfect secrecy are allowed. We used similar techniques to study the cryptographic power of a shared Cartesian reference frame, a type of physical information that cannot be established by any amount of discussion. Our main result was to find the optimal way to use such a reference frame to send private quantum data which was three times better than any previously discovered method.

2.4 Future goals

In the near future, we will investigate new applications to general two-party computations in a two-prover setting. We will identify several two-party protocols that could take advantage of our construction of a two-prover quantum bit commitment scheme. Moreover, our recent results left open certain questions of composability of two-prover protocols. We need to identify clearly the requirements of a quantum bit commitment scheme that is compatible with the construction of a quantum oblivious transfer (as was proposed by Crépeau and Kilian, and later proved secure by Yao). A somewhat similar investigation was realized in a computational setting by [45].

More general considerations about two-party quantum protocols will also be a major investigation. We currently know very little about two-party protocols on quantum data. We hope to unveil a number of basic elements that we later may compose. We already know how to commit to qubits if we have a primitive to commit classical bits. Definitions of appropriate notion of two-party quantum computations will be necessary to investigate eventual protocol to securely achieve them.

We plan to apply decoy state protocols [137] to “open air” QKD, as well as to study the security and practical feasibility of other quantum cryptographic and quantum communication protocols. If feasible, we will perform experimental demonstrations of those protocols. Examples include secret sharing of quantum states, orthogonal-state quantum cryptography, anonymous voting and surveying.

3 Theory of quantum information implementations

We have made significant progress in two areas: the theory of quantum error-correcting codes and fault-tolerant computation; and the study of specific physical technologies for building quantum information processing devices.

3.1 Quantum error correction

All implementations of quantum information processing are likely to include errors in one form or another. We have developed a methodology for quantum error correction for more general types of noise than were previously known by using a new way of producing codes. The rough idea is to “locate” the information not only in states but also in operators (i.e. mixed states). This work [120] unifies error correcting and error preventing schemes into a general framework which opens up a new way to make quantum information robust. (This work was recently publicized in the journal *Science* in an article called “Teaching Qubits New Tricks” in July, 2005.)

Also, the application of quantum error correction to quantum cryptography is an area where we have recently made progress by showing that quantum error correcting schemes can actually be applied with today’s technology [30]. In contrast with the case for quantum computation, quantum cryptography requires only that certain individual states be prepared, and it turns out that these can be reached with today’s technology when the information is encoded in the polarization of the photons. The group of Pan in China is presently implementing the simplest of the protocols.

We obtained much better understanding of various measurement-based models of quantum computation, that have connections with fault-tolerant computation. The one-way quantum computer model and the teleportation based model were derived from a single conceptual tool [7, 50]. We improved on the efficiency for simulating the elementary circuit operations in these measurement-based models. Subsequently, we also obtained a simple analysis of fault tolerance and lower bounds on the error threshold in these models, and proved that it is comparable to the circuit model in the so call graph-state model [8].

3.2 Physical models of quantum information

We have investigated a set of algorithms where the initial state is not a pure state but rather a pseudo-pure one for a single qubit and a completely mixed state for the others. What has been shown in the past is that there are algorithms that used this initial state which have no known polynomial classical algorithms. This is a surprising fact because of the high mixture of the initial state. One criticism of the work had been that these algorithms might not be particularly interesting. In a recent paper we showed that they could be used to distinguish between quantum systems whose evolution possess some symmetry (regular systems) and those who don’t (chaotic system). In the last year we have succeeded in implementing one of these algorithms in liquid state NMR.

We have addressed the important question of whether the efficiency of single photon generation can be enhanced by interferometry and postselection based on photon counting [29, 28]. Although the fundamental question is still open, this work established the mathematical foundations for treating the problem and established several theorems that can be used to answer the question in full generality contingent on solving one outstanding question.

Our research on quantum fingerprinting has been important because quantum fingerprinting can be far superior to its classical counterpart, because it is an outstanding example of quantum communication complexity, because of its amenability to experimental realization, and because of its potential to be a primitive for quantum authentication and other quantum information protocols [156, 157, 104]. Our goal is to make quantum fingerprinting experimentally realization for few-qubit systems, which requires a theory of mixed-state quantum fingerprinting. As quantum fingerprinting relies heavily on quantum measurement theory, a significant effort is underway to create theories for measuring and for comparing few-qubit mixed quantum states. In addition, we will collaborate closely with quantum optics experimentalists to realize these states in the laboratory.

We have implemented, measured, and analyzed the noise on a specific prototype quantum information processor [146, 167]. One important development from the analysis was our observation that in the presence of a certain type of quantum noise (i.e., “incoherent noise” due to uncontrolled variation of a classical control parameter), the standard QPT method fails to yield a completely positive linear map (which is normally the most general allowed quantum transformation) due to correlations in the errors associated with the input states and the actual transformation. In [146] we developed a perturbative method of analyzing the eigenvalues of the noisy transformation to measure the relative strength and other signatures of the incoherent noise affecting the implementation.

In this recent work [111] we have shown that the implementation of a random unitary transformation followed by its inverse gives an estimate of the overall noise strength affecting the physical implementation. The important feature of this protocol is that it requires only a constant number of experiments, and hence provides a useful alternative to quantum process tomography, where the number of experiments increases exponentially with the number of qubits.

3.3 Future goals

We wish to quantify the difficulty of maintaining the necessary reference frames for large scale quantum computations. We expect (and hope) that the difficulty scales polynomially in both the number of qubits and the number of gates, but wish to elucidate the techniques used in algorithmic language, and quantify the complexities. We plan to investigate the cavity QED model in detail, and expect our findings will apply to other implementations as well.

We will further investigate and develop the mathematical tools for new error protecting methods such as the one we have recently discovered but with focus on their application to specific quantum information processing devices.

We intend to develop pre-compilers, that are compilers and optimizers for implementing quantum algorithms for using nuclear magnetic resonance technology.

Continuous variable quantum information processing works with strong fields of light and may offer practical secure quantum communication beyond the reach of single- or few-photon implementations. We will address important problems concerning security of quantum key distribution with continuous variables, off-line resources for universal operations using only gaussian operations, and quantum algorithms for continuous variable quantum information processing.

4 Quantum information theory and entanglement theory

We have made significant progress in: the analysis of properties of entangled states; the quantum analogue of quantum Shannon Information Theory; and the development of a theory of pseudorandomness for quantum operations.

4.1 Entanglement theory

The paper [163] proves a fact about entanglement distillation that sheds some light on the difficult problem of characterizing the class of quantum states that can be distilled by physically separated parties that can communicate, but only classically. To say that entanglement is distilled means that it can be converted from a possibly complicated and noisy form into “useful”, near-perfect entanglement such as EPR-pairs that are used in quantum teleportation and other protocols. Specifically, the above paper proves that there exist rather peculiar states for which no useful entanglement whatsoever can be distilled until the number of copies of the given state passes a threshold, after which entanglement distillation is possible. This rules out some approaches to characterizing the states for which distillation is possible that were previously considered.

4.2 Quantum Shannon Theory

The papers [165, 164] study various properties of quantum channels. The paper [165] proves some facts about super-operator norms that were not known previously. Super-operator norms are useful when describing certain properties of quantum mechanical operations, and are closely related to some fundamental open question in quantum information theory. The paper [164] gives a constructive proof of the existence of a quantum channel with a property that is interesting in the context of corrected channel capacities.

We have continued our study of quantum two-way channels—bipartite quantum operations that can generate quantum and classical communication or entanglement between two parties. In the unitary case, we have found the a tradeoff involving quantum backward and forward-communication and entanglement in terms of that for classical communication [85].

In the non-unitary case, we obtained some bounds on the forward and backward classical communication tradeoff [49].

We have discovered new and better ways of communicating classical bits, quantum bits and entanglement. Some highlights include the discovery that when the sender of a quantum state is allowed to know which state she is sending, the famous teleportation protocol turns out *not* to be optimal. There is an improved method of communicating that uses only half as much quantum communication. Likewise, we have extended the well-known superdense coding protocol to the transmission of quantum states, demonstrating that in the limit of large messages, one ebit and one qubit of communication suffice to send a two qubit message.

In the past year, we have been working intensively on developing a theoretical foundation for the understanding of networks of quantum processors communicating through a noisy medium. This work has solved the problem of many senders sharing a noisy channel to a single receiver and made substantial progress on the opposite problem of a single sender communicating to many receivers. One of the major surprises has been the discovery that quantum data can be used as “side information” to help decode other quantum data in these scenarios. Various no-go theorems had suggested this would be impossible due to the inherent fragility of quantum information.

The study of distributed processing in quantum mechanics invariably leads to questions about the nature of entanglement and the resources required to transform a given state shared between two or more parties into a different state. Our accomplishments in this area include detailed necessary and sufficient conditions for one state to be convertible to another using limited quantum communication. The problem was found to be equivalent to a natural task in symplectic geometry, namely giving an explicit description of the “moment polytope” for a particular Hamiltonian group action.

4.3 Pseudorandom quantum operations

We have explored various techniques for constructing “pseudo-random” quantum operations. Several recent papers, including [111], have proposed randomization protocols where the implementation of a Haar-random unitary operator is assumed. However, the implementation of a Haar-random quantum transformation is extremely “hard”, in the sense that the number of gates grows exponentially with the number of qubits. These considerations have motivated recent studies of efficient methods for generating pseudo-random quantum transformations, that have several features of Haar-random ones, but are efficiently implementable. In an important recent paper [112], we reported numerical and experimental evidence suggesting that a “random circuit” (a sequence of randomly drawn gates) provides an efficient method for generating adequately pseudo-random transformations. The analytic features of the random circuit method were developed more fully in subsequent work [113], which provided a framework for determining whether efficient random circuits are sufficiently randomizing for any given task.

4.4 Future goals

The problem of characterizing the class of states that can be distilled as discussed above has been open for several years. One of our goals is to make further progress in better understanding the difficulty of this problem, with the hope of making progress toward resolving it. We also plan to continue to work on properties of quantum channels and super-operator norms in order to further develop the understanding of these objects.

We will continue the study of various communication protocols in the multiparty and nonunitary setting. We will also finalize the results on the composability security of encryption key recycling using authentication.

We will work to determine the capacities of quantum channels or networks composed of one or multiple senders, receivers, relay stations, and noise sources, to transmit quantum states and to perform other tasks. Understanding the basic limitations of such networks and designing protocols for achieving them could be a crucial precursor to building large-scale quantum computers, many proposals for which consist of networks of much smaller computers. I've already begun this effort, as described above, but a vast amount remains to be done. Perhaps most pressing, distributing quantum information over large distances will only be possible through the use of relay stations. Only rudimentary work has been done on the problem thus far and major improvements over existing protocols seems possible.

Many basic results in quantum information theory rely on concentration of measure effects. The methods used to prove the results, from operator Chernoff bounds to estimates of the concentration function for Riemannian manifolds, are beautiful but frequently get applied in a frustratingly ad hoc manner. More importantly, potentially powerful generalizations of existing results appear to be mathematically inaccessible at the moment due to the inadequacy of the present set of tools. For example, the *measurement compression theorem*, a fundamental building block of the theory of quantum information, nonetheless suffers from a crucial deficiency in its current form: the protocol must be tailored to the input states and, therefore, cannot be applied obliviously to arbitrary inputs. Freeing this theorem from its dependence on the input would pave the way for a true asymptotic theory of quantum *operations*. Ultimately, a single set of powerful tools should unify the current disparate proofs of the basic theorems of quantum information and allow us to greatly extend the theory.

Selected publications

- [1] D. W. Leung, A. Childs and H.-K. Lo. Two-way quantum communication channels. *arXiv:quant-ph/0506039*, 2005.
- [2] Scott Aaronson and Andris Ambainis. Quantum search of spatial regions. In *FOCS*, pages 200–209, 2003.

- [3] A. Abeyesinghe and P. Hayden. Generalized remote state preparation: Trading cbits, qubits and ebits in quantum communication. *Phys. Rev. A*, 68:062319.1–062319.9, 2003. arXiv:quant-ph/0308143.
- [4] A. Abeyesinghe, P. Hayden, G. Smith, and A. Winter. Optimal superdense coding of entangled states. arXiv:quant-ph/0407061. Accepted to *IEEE Trans. Inf. Th.*, 2005.
- [5] C. Ahn, A. Doherty, P. Hayden, and A. Winter. On the distributed compression of quantum information. arXiv:quant-ph/0403042. Accepted to *IEEE Trans. Inf. Th.*, 2005.
- [6] G. Ahokas, D. W. Berry, R. Cleve, and B. C. Sanders. Efficient quantum algorithms for simulating sparse hamiltonians. *quant-ph*, page 0508139, 2005.
- [7] P. Aliferis and D.W. Leung. Computation by measurements: A unifying picture. *Phys. Rev. A*, 70:062314, 2004. arXiv e-print quant-ph/0404082.
- [8] P. Aliferis and D.W. Leung. Fault-tolerant quantum computation with graph states, 2005. arXiv e-print quant-ph/0503130.
- [9] Andris Ambainis. Polynomial degree vs. quantum query complexity. In *FOCS*, pages 230–239, 2003.
- [10] Andris Ambainis. A new protocol and lower bounds for quantum coin flipping. *J. Comput. Syst. Sci.*, 68(2):398–416, 2004.
- [11] Andris Ambainis. Quantum walk algorithm for element distinctness. In *FOCS*, pages 22–31, 2004.
- [12] Andris Ambainis, Kazuo Iwama, Akinori Kawachi, Hiroyuki Masuda, Raymond H. Putra, and Shigeru Yamashita. Quantum identification of boolean oracles. In *STACS*, pages 105–116, 2004.
- [13] Andris Ambainis, Julia Kempe, and Alexander Rivosh. Coins make quantum walks faster. In *SODA*, pages 1099–1108, 2005.
- [14] Andris Ambainis, Leonard J. Schulman, Amnon Ta-Shma, Umesh V. Vazirani, and Avi Wigderson. The quantum communication complexity of sampling. *SIAM J. Comput.*, 32(6):1570–1585, 2003.
- [15] Andris Ambainis and Adam Smith. Small pseudo-random families of matrices: Derandomizing approximate quantum encryption. In *APPROX-RANDOM*, 2004.
- [16] A Tausz B. Qi, L. Qian and H.-K. Lo. Frequency-shifted mach-zehnder interferometer for locating multiple weak reflections along a fiber link. *Submitted to IEEE Photonics Technology Letters*, 2005.

- [17] L. Qian B. Qi, A. Tausz and H.-K. Lo. High-resolution, large dynamic range fiber length measurement based on frequency-shifted asymmetrical sagnac interferometer. *Accepted by Optics Letters*, 2005.
- [18] E. Bach, S. Coppersmith, M. Goldschen, R. Joynt, and J. Watrous. One-dimensional quantum walks with absorbing boundaries. *Journal of Computer and System Sciences*, 69(4):562–592, 2004.
- [19] H. Barnum, P. Hayden, R. Jozsa, and A. Winter. On the reversible extraction of classical information from a quantum source. *Proc. R. Soc. Lond. A*, 457:2019–2039, 2001. arXiv:quant-ph/0011072.
- [20] S. D. Bartlett, P. Hayden, and R. W. Spekkens. Random subspaces for encryption based on a private shared Cartesian frame. arXiv:quant-ph/0506260. Accepted to *Phys. Rev. A*, 2005.
- [21] Jonathan Baugh, Osama Moussa, Colm Ryan, Ashwin Nayak, and Raymond Laflamme. A spin-based heat engine: Experimental implementation of heat-bath algorithmic cooling. *Nature*. Provisionally accepted, 2005.
- [22] M. Ben-Or, M. Horodecki, D. Leung, D. Mayers, and J. Oppenheim. The universal composable security of quantum key distribution. In *Theory of Cryptography Conference, LNCS 3378*, Ed. J. Kilian, volume 3378, pages 386–406, 2005. arXive e-print quant-ph/0409078.
- [23] S. C. Benjamin and P. Hayden. Comment on ‘Quantum games and quantum strategies’. *Phys. Rev. Lett.*, 87(6):069801.1, 2001. arXiv:quant-ph/0003036.
- [24] S. C. Benjamin and P. Hayden. Multi-player quantum games. *Phys. Rev. A*, 64(3):030301.1–030301.4, 2001. arXiv:quant-ph/0007038.
- [25] C. H. Bennett, P. Hayden, D. W. Leung, P. W. Shor, and A. Winter. Remote preparation of quantum states. *IEEE Trans. Inf. Th.*, 51(1):56–74, 2005. arXiv:quant-ph/0307100.
- [26] D. W. Berry, A. I. Lvovsky, and B. C. Sanders. Interconvertibility of single-rail optical qubits. *Optics Letters (accepted)*, 2005.
- [27] D. W. Berry, S. Scheel, C. R. Myers, B. C. Sanders, P. L Knight, and R. Laflamme. Improving single photon sources via linear optics and photodetection. In *Proceedings of the Conference on Fluctuations and Noise in Photonics and Quantum Optics II*, volume 5468 of *AIP Proceedings*, pages 25–28, Gran Canaria, Spain, May 2004. SPIE’s First International Symposium on Optical Science and Technology.
- [28] D. W. Berry, S. Scheel, C. R. Myers, B. C. Sanders, P. L. Knight, and R. Laflamme. Post-processing with linear optics for improving the quality of single-photon sources. *New Journal of Physics*, 6(4), 2004.

- [29] D. W. Berry, S. Scheel, B. C. Sanders, and P. L. Knight. Improving single-photon sources via linear optics and photodetection. *Physical Review A*, 69(3), March 2004.
- [30] J.-C. Boileau, D. Gottesman, R. Laflamme, D. Poulin, and R.W. Spekkens. Robust polarization-based quantum key distribution over collective-noise channel. *Physical Review Letters*, 92:17901, 2004.
- [31] J.-C. Boileau, R. Laflamme M. Laforest, and C. R. Myers. Robust quantum communication using a polarization-entangled photon pair. *Physical Review Letters*, 93:220501, 2005.
- [32] J.-C. Boileau, K. Tamaki, J. Batuwantudawe, and R. Laflamme. Higher security thresholds for quantum key distribution by improved analysis of dark counts. 2005. quant-ph/0502140.
- [33] J.-C. Boileau, K. Tamaki, J. Batuwantudawe, and R. Laflamme. Unconditional security of three state quantum key distribution protocols. *Physical Review Letters*, 94:040503, 2005.
- [34] M. D. Bowdrey, J. A. Jones, E. Knill, and R. Laflamme. Compiling gate networks on an ising quantum computer. *Physical Review A*, page 032315, 2005. quant-ph/0506006.
- [35] G. Brassard, A. Broadbent, and A. Tapp. Quantum pseudo-telepathy. *Foundations of Physics*, 35(11), November 2005.
- [36] G. Brassard, A. Broadbent, and A. Tapp. Recasting mermin’s multi-player game into the framework of pseudo-telepathy. *Quantum Information and Computation (QIC)*, 35(7), November 2005.
- [37] G. Brassard, A. A. Methot, and A. Tapp. Minimum entangled state dimension required for pseudo-telepathy. *Foundations of Physics*, 5(4), 2005.
- [38] Anne Broadbent and Andr Allan Mthot. On the power of non-local boxes. *Theoretical Computer Science*, To appear.
- [39] T. Brun, H. Klauck, A. Nayak, M. Rötteler, and C. Zalka. Comment on “probabilistic quantum memories”. *Physical Review Letters*, 91(20):article 209801, 2003.
- [40] Todd A Brun, Hilary A Carteret, and Andris Ambainis. The quantum to classical transition for random walks. *Physical Review Letters*, 91:130602, 2003.
- [41] Todd A Brun, Hilary A Carteret, and Andris Ambainis. Quantum walks driven by many coins. *Physical Review A*, 67:052317, 2003.
- [42] H. Buhrman, M. Christandl, P. Hayden, H.-K. Lo, and S. Wehner. On the (im)possibility of quantum string commitment. arXiv:quant-ph/0504078, 2005.

- [43] Harry Buhrman, Christoph Dürr, Mark Heiligman, Peter Høyer, Frédéric Magniez, Miklos Santha, and Ronald de Wolf. Quantum algorithms for element distinctness. *SIAM Journal on Computing*, 34(6):1324–1330, 2005.
- [44] Harry Buhrman, Peter Høyer, Serge Massar, and Hein Röhrig. Combinatorics and quantum nonlocality. *Physical Review Letters*, 91:047903, 2003.
- [45] D. Mayers C. Crépeau, P. Dumais and L. Salvail. Computational collapse of quantum state with application to oblivious transfer. In *proceedings of the 1st Theoretical Cryptography Conference*, volume 2951 of *Lecture Notes in Computer Science*, pages 374–393. Springer-Verlag, 2004.
- [46] C. Negreverne D. Poulin R. Laflamme C. Ryan, J. Emerson. Characterisation of complex dynamics on a scalable quantum processor.
- [47] K. Chen and H.-K. Lo. Multi-partite quantum cryptographic protocols with noisy ghz states,. <http://xxx.lanl.gov/abs/quant-ph/0404133>, 2004.
- [48] K. Chen and H.-K. Lo. Conference key agreement and quantum sharing of classical secrets with noisy ghz states. *IEEE ISIT (International Symposium on Information Theory) 2005*, 2005.
- [49] A. Childs, D. Leung, and H.-K. Lo. Two-way quantum communication channels, 2005. arXive e-print quant-ph/0506039.
- [50] A. Childs, D.W. Leung, and M. Nielsen. Unified derivations of measurement-based schemes for quantum computation. *Phys. Rev. A*, 71:032318, 2005. arXive e-print quant-ph/0404132.
- [51] R. Cleve, P. Høyer, B. Toner, and J. Watrous. Consequences and limits of nonlocal strategies. In *Proceedings of the 19th Annual IEEE Conference on Computational Complexity*, pages 236–249, 2004.
- [52] Richard Cleve, Peter Høyer, Benjamin Toner, and John Watrous. Consequences and limits of nonlocal strategies. In *Proceedings of the 19th IEEE Annual Conference on Computational Complexity*, pages 236–249, 2004.
- [53] C. Crépeau, J.-R. Simard, and A. Tapp.
- [54] Claude Crépeau, Jean-Raymond Simard, and Alain Tapp. Classical and quantum strategies for two-prover bit commitments. In *submitted to STOC06*.
- [55] N. Lutkenhaus D. Gottesman, H.-K. Lo and J. Preskill. Security of quantum key distribution with imperfect devices. *IEEE ISIT (International Symposium on Information Theory) 2004*, 2004.

- [56] S. Daftuar and P. Hayden. Quantum state transformations and the Schubert calculus. *Ann. Phys.*, 315(1):80–122, 2005. arXiv:quant-ph/0410052.
- [57] J. Niel de Beaudrap. Applying quantum information to fingerprinting schemes and algebraic structures. Master’s thesis, University of Calgary, Calgary, Alberta, Canada, 2004.
- [58] J. Niel de Beaudrap. One-qubit fingerprinting schemes. *Physical Review A*, 69:article 022307, 2004.
- [59] D. Deutsch and P. Hayden. Information flow in entangled quantum systems. *Proc. R. Soc. Lond. A*, 456(1999):1759–1774, 2000. arXiv:quant-ph/9906007.
- [60] D. P. DiVincenzo, P. Hayden, and B. M. Terhal. Hiding quantum data. *Found. Phys.*, 33(11):1629–1647, 2003. arXiv:quant-ph/0207147. Invited contribution to ‘David Mermin Festschrift’.
- [61] D. P. DiVincenzo, M. Horodecki, D. Leung, J. Smolin, and B. M. Terhal. Locking classical correlation in quantum states. *Phys. Rev. Lett.*, 92:067902, 2004. arXiv e-print quant-ph/0303088.
- [62] A. Ekert, M. Ericsson, P. Hayden, H. Inamori, J. A. Jones, D. K. L. Oi, and V. Vedral. Geometric quantum computation. *J. Mod. Opt.*, 47(14-15):2501–2513, 2000. arXiv:quant-ph/0004015.
- [63] A. Ekert, P. Hayden, and H. Inamori. Basic concepts in quantum computation. In R. Kaiser, C. Westbrook, and F. David, editors, *Proceedings of the 1999 Les Houches summer school on ‘Coherent matter waves’*, volume 72, pages 661–703, 2001. arXiv:quant-ph/0011013.
- [64] A. Ekert, P. Hayden, H. Inamori, and D. K. Oi. What is quantum computation? *J. Mod. Phys. A*, 16(20):3335–3363, 2001. (Not posted to arXiv.)
- [65] Mark Ettinger, Peter Høyer, and Emanuel Knill. The quantum query complexity of the hidden subgroup problem is polynomial. *Information Processing Letters*, 91(1):43–48, 16 July 2004.
- [66] B. Fortescue and H.-K. Lo. Inefficiency and classical communication bounds for conversion between partially entangled pure bipartite states. *Physical Review A*, 72, 2005.
- [67] B. Fortescue and H.-K. Lo. Inefficiency and classical communication bounds for conversions between partially entangled pure bipartite quantum states. *IEEE ISIT (International Symposium on Information Theory) 2005*, 2005.
- [68] C.C. Lopez J. Emerson J.P. Paz T.F. Havel G. Teklemariam, E. Fortunato and D. Cory. Method for modelling decoherence on a quantum information processor.

- [69] V. Galliard, A. Tapp, and S. Wolf. The impossibility of pseudo-telepathy without quantum entanglement. In *Proceedings of the 2003 IEEE International Symposium on Information Theory (ISIT03)*, 2003.
- [70] H. Gerhardt and J. Watrous. Continuous-time quantum walks on the symmetric group. In *Proceedings of the 7th International Workshop on Randomization and Approximation Techniques in Computer Science*, volume 2764 of *Lecture Notes in Computer Science*, pages 290–301. Springer-Verlag, 2003.
- [71] S. Ghose, P. M. Alsing, I. H. Deutsch, and B. C. Sanders. The quantum to classical transition in entangled systems via continuous measurements. In *The Seventh International Conference on Quantum Communication, Measurement and Computing*, volume 734 of *AIP Proceedings*, pages 61–66, Glasgow, United Kingdom, July 2004. SPIE Annual Meeting.
- [72] S. Ghose, P. M. Alsing, B. C. Sanders, and I. H. Deutsch. Entanglement and the quantum-to-classical transition. *Physical Review A*, 72(1):014102, July 2005.
- [73] S. Ghose and B. C. Sanders. Entanglement dynamics in chaotic systems. *Physical Review Letters*, 70(6):062315, December 2004.
- [74] S. Ghose and B. C. Sanders. Analysis of non-gaussian states of light as a resource for quantum information processing with continuous variables. In *Proceedings of the Conference on Quantum Communications and Quantum Imaging III*, volume 5893, San Diego, August 2005. SPIE Annual Meeting.
- [75] A. Golynski and P. Sen. A note on the power of quantum fingerprinting. ArXiv preprint quant-ph/0510091, 2005.
- [76] Daniel Gottesman and Hoi-Kwong Lo. From quantum cheating to quantum security. *Physics Today*, 53:22, 2000.
- [77] Daniel Gottesman and Hoi-Kwong Lo. Proof of security of quantum key distribution with two-way classical communications. *IEEE Transactions on Information Theory*, 49:457, 2003.
- [78] Daniel Gottesman, Hoi-Kwong Lo, Norbert Lutkenhaus, and John Preskill. Security of quantum key distribution with imperfect devices. *Quantum Information and Computation*, 4:325, 2004.
- [79] G. Gour, D. A. Meyer, and B. C. Sanders. Deterministic entanglement of assistance and monogamy constraints. *Physical Review A (in press)*, 2005.
- [80] G. Gour and B. C. Sanders. Remote preparation and distribution of bipartite entangled states. *Physical Review Letters*, 93(26):260501, December 2004.

- [81] G. Gutoski. Upper bounds for quantum interactive proofs with competing provers. In *Proceedings of the 20th Annual IEEE Conference on Computational Complexity*, pages 334–343, 2005.
- [82] G. Gutoski and J. Watrous. Quantum interactive proofs with competing provers. In *Proceedings of the 23rd International Symposium on Theoretical Aspects of Computer Science*, volume 3404 of *Lecture Notes in Computer Science*, pages 605–616. Springer-Verlag, 2005.
- [83] P. Hayden H.-K. Lo S. Wehner H. Buhrman, M. Christandl. On the (im)possibility of quantum string commitment,. <http://arxiv.org/abs/quant-ph/0504078>, 2005.
- [84] A. Harrow, P. Hayden, and D. W. Leung. Superdense coding of quantum states. *Phys. Rev. Lett.*, 92:187901.1–187901.4, 2004. arXiv:quant-ph/0307221.
- [85] A. Harrow and D. Leung. Bidirectional coherent classical communication. *Quant. Inf. Comp.*, 5:380–395, 2005. arXiv e-print quant-ph/0412126.
- [86] A. Harrow and H.-K. Lo. A tight lower bound on the classical communication cost of entanglement dilution. *IEEE Transactions on Information Theory*, 50:319, 2004.
- [87] A. W. Harrow and H. K. Lo. A tight lower bound on the classical communication cost of entanglement dilution. *IEEE ISIT (International Symposium on Information Theory) 2003*, 2003.
- [88] P. Hayden. Putting certainty in the bank.
- [89] P. Hayden. Entanglement in random subspaces. In *Proceedings of the Seventh International Conference on Quantum Communication, Measurement and Computing*, pages 226–229. American Institute of Physics, 2004. arXiv:quant-ph/0409157.
- [90] P. Hayden. Capacities enhanced by entanglement. To appear in the *Encyclopedia of Mathematical Physics*, Elsevier, 2005.
- [91] P. Hayden, M. Horodecki, and B. M. Terhal. The asymptotic entanglement cost of preparing a quantum state. *J. Phys. A*, 34(35):6891–6898, 2001. arXiv:quant-ph/0008134.
- [92] P. Hayden, R. Jozsa, D. Petz, and A. Winter. Structure of states which satisfy strong subadditivity of quantum entropy with equality. *Commun. Math. Phys.*, 246(2):359–374, 2004. arXiv:quant-ph/0304007.
- [93] P. Hayden, R. Jozsa, and A. Winter. Trading quantum for classical resources in quantum data compression. *J. Math. Phys.*, 43(9):4404–4444, 2002. arXiv:quant-ph/0204038.

- [94] P. Hayden and C. King. Correcting quantum channels by measuring the environment. *Quantum information and computation*, 5(2):156–160, 2005. arXiv:quant-ph/0409026.
- [95] P. Hayden, D. Leung, and G. Smith. Multiparty data hiding of quantum information. *Phys. Rev. A*, 71:062339, 2005. arXiv e-print quant-ph/0407152.
- [96] P. Hayden, D. W. Leung, P. W. Shor, and A. Winter. Randomizing quantum states: Constructions and applications. *Commun. Math. Phys.*, 250(2):371–391, 2004. arXiv:quant-ph/0307104.
- [97] P. Hayden, D. W. Leung, and G. Smith. Multiparty data hiding of quantum information. *Phys. Rev. A*, 71:062339.1–062339.9, 2005. arXiv:quant-ph/0407152.
- [98] P. Hayden, D. W. Leung, and A. Winter. Aspects of generic entanglement. arXiv:quant-ph/0407049. Submitted to *Commun. Math. Phys.*, 2005.
- [99] P. Hayden, B. M. Terhal, and A. Uhlmann. On the LOCC classification of bipartite density matrices. arXiv:quant-ph/0011095, 2000.
- [100] P. Hayden and A. Winter. On the communication cost of entanglement transformations. *Phys. Rev. A*, 67:012326.1–012326.8, 2003. arXiv:quant-ph/0204092.
- [101] J.A. Holbrook, D.W. Kribs, and R. Laflamme. Noiseless subsystems and the structure of the commutant in quantum error correction. *Quantum Information Processing*, 2:381–419, 2003.
- [102] J.A. Holbrook, D.W. Kribs, R. Laflamme, and D. Poulin. Noiseless subsystems for collective rotation channels in quantum information theory. 2004.
- [103] R.T. Horn, S. A. Babichev, K.-P. Marzlin, A. I. Lvovsky, and B. C. Sanders. Single qubit optical quantum fingerprinting. *Physical Review Letters*, 95(15):150502, October 2004.
- [104] R.T. Horn, A. J. Scott, J. Walgate, R. Cleve, A. I. Lvovsky, and B. C. Sanders. Classical and quantum fingerprinting with shared randomness and one-sided error. *Quantum Information and Computation*, 5(3):258–271, May 2005.
- [105] Peter Høyer. The phase matrix. In *Proceedings of the 16th International Symposium on Algorithms and Computation*, Lecture Notes in Computer Science, page To appear, 2005.
- [106] Peter Høyer and Robert Špalek. Lower bounds on quantum query complexities. *Bulletin of the European Association for Theoretical Computer Science*, 87:78–103, October 2005.
- [107] Peter Høyer and Robert Špalek. Quantum fan-out is powerful. 1:81–103, 2005.

- [108] Peter Høyer and Robert Špalek. Tight adversary bounds for composite functions, September 2005.
- [109] Yuki Kelly Itakura. Quantum algorithm for commutativity testing of a matrix set. Master's thesis, University of Waterloo, Waterloo, Ontario, Canada, September 2005.
- [110] D. Poulin D. Cory J. Emerson, S. Lloyd. Estimation of the local density of states on a quantum computer.
- [111] K. Zyczkowski J. Emerson, R. Alicki. Scalable noise estimation with random unitary operators.
- [112] M. Saraceno S. Lloyd D. Cory J. Emerson, Y. Weinstein. Pseudo-random unitary operators for quantum information processing. 302:2098, 2003.
- [113] S. Lloyd J. Emerson, E. Livine. Convergence conditions for random quantum circuits.
- [114] S. Lloyd D. Cory J. Emerson, Y. Weinstein. Fidelity decay as an efficient indicator of quantum chaos. *Phys. Rev. Lett.*, 89:284102.
- [115] R. Jain, J. Radhakrishnan, and P. Sen. Prior entanglement, message compression and privacy in quantum communication. In *IEEE Conference on Computational Complexity*, pages 285–296, 2005.
- [116] V. Kendon and B. C. Sanders. Complementarity in quantum walks. In *The Seventh International Conference on Quantum Communication, Measurement and Computing*, volume 734 of *AIP Proceedings*, pages 133–138, Glasgow, United Kingdom, July 2004. SPIE Annual Meeting.
- [117] V. Kendon and B. C. Sanders. Complementarity and quantum walks. *Physical Review A*, 71(2):022307/1–022307/7, February 2005.
- [118] Iordanis Kerenidis and Ashwin Nayak. Weak coin flipping with small bias. *Information Processing Letters*, 89(3):131–135, February 2004.
- [119] Hartmut Klauck, Ashwin Nayak, Amnon Ta-Shma, and David Zuckerman. Interaction in quantum communication. *IEEE Transactions on Information Theory*. Submitted.
- [120] D. Kribs, R. Laflamme, and D. Poulin. A unified and generalized approach to quantum error correction. *Physical Review Letters*, 94:180501, 2005.
- [121] D. Kribs, R. Laflamme, D. Poulin, and M. Lesosky. Operator quantum error correction. 2005. quant-ph/0504189.
- [122] D. W. Leung. Quantum computation by measurements. *Int. J. Q. Info.*, 2:33–43, 2004. arXive e-print quant-ph/0310189.

- [123] H.-K. Lo. Proof of unconditional security of six-state quantum key distribution scheme. *Quantum Information and Computation*, 1:81, 2001.
- [124] H.-K. Lo. A simple proof of the unconditional security of quantum key distribution. *J. of Phys. A*, 34:6957, 2001.
- [125] H.-K. Lo. Method for decoupling error correction from privacy amplification. *New Journal of Physics*, 5:36, 2003.
- [126] H.-K. Lo and H. F. Chau. Is quantum bit commitment really possible? *Physical Review Letters*, 78:3410, 1997.
- [127] H.-K. Lo and T.-M. Ko. Some attacks on quantum-based cryptographic protocols. *Quantum Information and Computation*, 5:40, 2005.
- [128] H.-K. Lo and S. Popescu. Classical communication cost of entanglement manipulation: Is entanglement an interconvertible resource? *Physical Review Letters*, 83:1459, 1999.
- [129] H.-K. Lo and J. Preskill. Phase randomization improves the security of quantum key distribution.,. <http://arxiv.org/abs/quant-ph/0504209>, 2005.
- [130] Hoi-Kwong Lo. Classical-communication cost in distributed quantum-information processing: a generalization of quantum-communication complexity. *Physical Review A*, 62:012313, 2000.
- [131] Hoi-Kwong Lo. Cryptography's quantum barrier. *Physics World*, 2001.
- [132] Hoi-Kwong Lo. Error correction and security in quantum cryptography. *IEEE ISIT (International Symposium on Information Theory) 2003*, 2003.
- [133] Hoi-Kwong Lo. Quantum key distribution with vacua and dim pulses as decoy states. *IEEE ISIT (International Symposium on Information Theory) 2004*, 2004.
- [134] Hoi-Kwong Lo. Getting something out of nothing. *Quantum Information and Computation*, 4:413, 2005.
- [135] Hoi-Kwong Lo and H. F. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283:2050, 1999.
- [136] Hoi-Kwong Lo, H. F. Chau, and M. Ardehali. Efficient quantum key distribution scheme and proof of its unconditional security. *Journal of Cryptology*, 18:133, 2005.
- [137] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Physical Review Letters*, 94:230504, 2005.
- [138] Hoi-Kwong Lo and Sandu Popescu. Concentrating entanglement by local actions: Beyond mean values. *Physical Review A*, 63:022301, 2001.

- [139] Hoi-Kwong Lo, Tim Spiller, and Sandu Popescu. *Introduction to quantum computation and information*. World Scientific, Singapore, 1998.
- [140] J. Emerson A. Farid E. Fortunato T. F. Havel D. Cory M. A. Pravia, N. Boulant. Robust control of quantum information.
- [141] Xiongfeng Ma, Bing Qi, Yi Zhao, and Hoi-Kwong Lo. Practical decoy state for quantum key distribution. *Physical Review A*, 72:012326, 2005.
- [142] Frédéric Magniez and Ashwin Nayak. Quantum complexity of testing group commutativity. *Algorithmica*. Submitted.
- [143] Frédéric Magniez and Ashwin Nayak. Quantum complexity of testing group commutativity. In *Proceedings of the 32nd International Colloquium on Automata, Languages and Programming*, Lecture Notes in Computer Science, pages 1312–1324. Springer-Verlag, July 11–15 2005. Lisboa, Portugal.
- [144] C. Marriott and J. Watrous. Quantum arthur-merlin games. *Computational Complexity*, 14(2):122–152, 2005.
- [145] M. Mosca and C. Zalka. Exact quantum fourier transforms and discrete logarithm algorithms. In *ERATO Conference on Quantum Information Science 2003 (EQIS 2003)*, 2005.
- [146] J. Emerson T. F. Havel D. Cory N. Boulant, S. Furuta. Incoherent noise and quantum control.
- [147] Ashwin Nayak and Julia Salzman. Limits on the ability of quantum states to convey classical messages. *Journal of the ACM*. Accepted, 2005.
- [148] N. Boulant C. Ramanathan S. Lloyd D. G. Cory P. Cappellaro, J. Emerson. Entanglement assisted metrology. *Phys. Rev. Lett.*, 94:020502.
- [149] J. Radhakrishnan, M. Rötteler, and P. Sen. On the power of random bases in fourier sampling: Hidden subgroup problem in the heisenberg group. In *Proceedings of the 32nd International Colloquium on Automata, Languages and Programming (ICALP)*, volume 3580 of *Lecture Notes in Computer Science*, pages 1399–1411. Springer-Verlag, 2005.
- [150] B. Rosgen and J. Watrous. On the hardness of distinguishing mixed-state quantum computations. In *Proceedings of the 20th Annual Conference on Computational Complexity*, pages 344–354, 2005.
- [151] C.A. Ryan, J. Emerson, D. Poulin, C. Negrevergne, and R. Laflamme. Characterization of complex quantum dynamics with a scalable nmr information processor. *Physical Review Letters*, to appear, 2005.

- [152] D.Gottesman S. L. Braunstein, C. A. Fuchs and H.-K. Lo. A quantum analog of huffman coding. *IEEE Transactions on Information Theory*, 46:1644, 2000.
- [153] B. C. Sanders. Classical vs quantum fingerprinting. In IEEE Computer Society, editor, *The Thirty-Fifth International Symposium on Multiple-Valued Logic (ISMVL 2005)*, pages 1–4, Tokyo, May 2005. University of Calgary.
- [154] B. C. Sanders and S. Bandyopadhyay. Concatenated quantum teleportation? In *Proceedings of the Conference on Quantum Communications and Quantum Imaging III*, volume 5893, San Diego, August 2005. SPIE Annual Meeting.
- [155] B. C. Sanders, G. Gour, and D. A. Meyer. Remote entanglement distribution and entanglement of assistance. In *ERATO Conference on Quantum Information Science 2005 (EQIS 2005)*, 2005.
- [156] B. C. Sanders, R. Horn, and K.-P. Marzlin. Single-qubit optical quantum fingerprinting. In *Proceedings of the Conference on Quantum Communications and Quantum Imaging II*, volume 5551 of *AIP Proceedings*, pages 137–143, Denver, August 2004. SPIE Annual Meeting.
- [157] A. J. Scott, J. Walgate, and B. C. Sanders. Optimal fingerprinting strategies with one-sided error. *quant-ph*, page 0507048, 2005.
- [158] K. Tamaki and H.-K. Lo. Quantum key distribution: Beyond no-cloning theorem. <http://arxiv.org/abs/quant-ph/0412035>, 2004.
- [159] K. Tamaki and H.-K. Lo. Unconditionally secure key distillation from multi-photons in a single-photon polarization-based quantum key distribution. *IEEE ISIT (International Symposium on Information Theory) 2005*, 2005.
- [160] W. van Dam and P. Hayden. Renyi-entropic bounds on quantum communication. arXiv:quant-ph/0204093.
- [161] W. van Dam and P. Hayden. Embezzling entangled quantum states (in press as *Universal entanglement transformations without communication*). *Phys. Rev. A*, 67(6):060302.1–060302.3, 2003. arXiv:quant-ph/0201041.
- [162] X. Wang, S. Ghose, B. C. Sanders, and B. Hu. Entanglement as a signature of quantum chaos. *Physical Review E*, 70(1):16217–1–8, July 2004.
- [163] J. Watrous. Many copies may be required for entanglement distillation. *Physical Review Letters*, 93(1): article 010502, 2004.
- [164] J. Watrous. Bipartite subspaces having no bases distinguishable by local operations and classical communication. *Physical Review Letters*, 95(8): article 080505, 2005.

- [165] J. Watrous. Notes on super-operator norms induced by Schatten norms. *Quantum Information and Computation*, 5(1):58–68, 2005.
- [166] J. Emerson D. Cory Y. Weinstein, S. Lloyd. Experimental implementation of the quantum baker’s map. *Phys. Rev. Lett.*, 89:157902.
- [167] J. Emerson N. Boulant M. Saraceno D. Cory Y. Weinstein, T. F. Havel. Quantum process tomography of the quantum fourier transform.
- [168] X. Ma H.-K. Lo Y. Zhao, B. Qi and L. Qian. Experimental quantum key distribution with decoy states. <http://arxiv.org/abs/quant-ph/0503192>, 2005.
- [169] J. Yard, I. Devetak, and P. Hayden. Capacity theorems for quantum multiple access channels. In *Proceedings of the 2005 IEEE Symposium on Information Theory, Adelaide, Australia*, pages 884–888, September 2005.
- [170] J. Yard, I. Devetak, and P. Hayden. Capacity theorems for quantum multiple access channels - part I: Classical-quantum and quantum-quantum capacity regions. arXiv:quant-ph/0501045, 2005.
- [171] J. Yard, I. Devetak, and P. Hayden. Quantum broadcast channels. In *Proceedings of the ERATO conference on Quantum Information Science, Tokyo, Japan*, pages 3–4, August 2005.
- [172] J. Yard, I. Devetak, and P. Hayden. Sending classical and quantum information over quantum multiple access channels. In *Proceedings of the Ninth Canadian Workshop on Information Theory, Montreal, Canada*, pages 387–390, June 2005.