Research Statement

Bill Fefferman, University of Maryland/NIST

Since the discovery of Shor's algorithm in the mid 1990's, it has been known that quantum computers can efficiently solve integer factorization, a problem of great practical relevance with no known efficient classical algorithm [1]. The importance of this result is impossible to overstate: the conjectured intractability of the factoring problem provides the basis for the security of the modern internet. However, it may still be a few decades before we build universal quantum computers capable of running Shor's algorithm to factor integers of cryptographically relevant size. In addition, we have little *complexity theoretic* evidence that factoring is computationally hard. Consequently, Shor's algorithm can only be seen as the first step toward understanding the power of quantum computation, which has become one of the primary goals of theoretical computer science.

My research focuses not only on understanding the power of quantum computers of the indefinite future, but also on the desire to develop the foundations of computational complexity to rigorously analyze the capabilities and limitations of present-day and near-term quantum devices which are not yet fully scalable quantum computers. Furthermore, I am interested in using these capabilities and limitations to better understand the potential for cryptography in a fundamentally quantum mechanical world.

1 Comparing quantum and classical nondeterministic computation

Starting with the foundational paper of Bernstein and Vazirani it has been conjectured that quantum computers are capable of solving problems whose solutions cannot be found, or even verified efficiently on a classical computer [2]. In particular, they conjecture the existence of an oracle problem solvable by efficient quantum computation that cannot be solved in NP, or even more generally, by the Polynomial-time Hierarchy, or PH. This has since become one of the most important and central questions in quantum complexity theory (see *e.g.,* [3, 4, 5]).

We have developed the only currently feasible route toward validating this conjecture via a novel connection between quantum algorithms and classical *pseudorandom generators* [6, 7]. These are classical algorithms that take a small number of uniformly random input bits and produce a much longer output that cannot be distinguished from uniform with a classical computer. We show that the output distribution of a particular instantiation of the ubiquitous Nisan-Wigderson pseudorandom generator [8] *can* be distinguished from the uniform distribution with a quantum computer. Likewise, we prove that these distributions cannot be distinguished by any NP algorithm. Proving that this distribution cannot be distinguished from uniform by any PH algorithm would fully confirm the conjecture of Bernstein and Vazirani, and has been a major goal in my research. In addition to the obvious quantum motivation, we have discovered new connections between attaining this separation and the development of pseudorandom generators with stronger parameters and new methods for proving *classical* circuit lower bounds (see [7]).

2 Quantum advantage from sampling experiments

An exciting line of work has established the existence of distributions samplable by quantum computers that cannot be sampled *exactly* by randomized classical computation, under mild hardness assumptions [9, 10]. Crucially, these results hold even for restrictive quantum samplers that are not universal quantum computers. As such, it is plausible that present-day laboratory devices are *already capable* of harnessing quantum effects to demonstrate computational tasks that are beyond the reach of even the fastest classical computers.

In the popular BosonSampling proposal, for example, such a sampling task is achieved by producing single photons, sending them through a network of beamsplitters and phase shifters, and performing photon-number resolving measurements [11]. A number of experimental groups have now performed demonstrations of small-scale BosonSampling experiments [12, 13, 14, 15, 16, 17].

However, the theory has not completely caught up with the experiment. While the photonic platform for quantum information processing has much in its favor, it suffers from imperfect detector efficiency and photon loss which gets worse as the number of optical components is scaled up. It is not understood whether the hardness-of-sampling proofs can be generalized to apply to experimentally realistic parameter regimes (see *e.g.,* [11, 18, 19, 20, 21]). To model experimental error, one would at least want an "approximate hardness" result ruling out efficient classical sampling from *any distribution* close in total variation distance to the ideal quantum distribution. In the case of BosonSampling, hardness of approximate sampling can only be obtained under unproven complexity theoretic hardness assumptions about the hardness of approximating the Permanent.

My interest in this line of work is multifaceted. I would like to understand the minimal hardness assumption needed to obtain strong approximate sampling results. We showed that a very simple quantum algorithm that applies some classical computation in quantum superposition followed by a quantum Fourier transform is capable of sampling from distributions that cannot be sampled approximately classically, under any of a broad array of hardness assumptions that formally weakens those needed by BosonSampling [22]. **This result provides the strongest provable evidence for the superiority of quantum computation under some of the weakest assumptions.** In future work, I hope to use surprising similarities between this quantum Fourier sampling distribution and the BosonSampling distribution to develop new methods for the *verification* of BosonSampling experiments.

Thinking about these sampling results led me to consider alterative physical systems capable of outperforming classical computation. Very recently, we showed that sampling from the output distribution of a different experimentally realizable quantum system (namely, an Ising model with no transverse field), is hard classically [23]. This result has already had theoretical implications concerning the complexity theoretic classification of two qubit commuting Hamiltonians [24].

3 Characterizing the power of quantum computation with restricted resources

Long before we see fully scalable quantum computers, we will have quantum devices with restricted resources. Theoretical models motivated by the limitations of real-world experiments involve restricting the standard quantum circuit model either in time (gate count), in space (number of qubits) or in depth.

Ta-Shma gave the first evidence that quantum computers could attain a quadratic advantage in space usage over classical computation, which is known to be the maximum possible [25, 26]. In particular, he demonstrated an algorithm for "well-conditioned" matrix[1] inversion, that runs in quantum $O(\log n)$-space.

Quantum algorithms for matrix inversion are of direct interest due to their many applications in scientific computing. Recent work has investigated applications of matrix inversion to problems ranging from machine learning [27], to calculation of radar scattering crossections [28]. The performance advantages of these quantum algorithms over classical computation are not well understood [29], a situation that could be improved by research into the complexity-theoretic foundations of space-limited quantum computation.

We recently gave another reason to care about the matrix inversion problem: it *completely characterizes* quantum space complexity. In particular we show that a

[1] A well-conditioned $n \times n$ matrix is one in which the condition number, or ratio between largest to smallest singular value, is bounded by a polynomial in n.

suitably parameterized matrix inversion problem is the hardest problem solvable by unitary quantum circuits that act on a bounded number of qubits. To do this, we improve on Ta-Shma's result both by giving a new algorithm for space efficient matrix inversion (avoiding the need for intermediate measurements) and by showing a matching hardness result [30, 31, 32]. This characterization is interesting, as the ability to invert certain other classes of matrices has been shown to be equivalent in power to quantum computation with bounded time [33]. Consequently, one can use the matrix inversion problem to give a direct comparison of the power of space-bounded quantum computations to time-bounded quantum computations, and explore how these resources trade off.

I am very interested in using these results, possibly together with results about quantum depth vs time and space tradeoffs (see *e.g.,* [34, 35]), to characterize the power of quantum computation with restricted depth. The desire to analyze the power of quantum depth is motivated experimentally, where the effects of decoherence make reliably implementing a quantum circuit with more than a small number of layers very challenging (see *e.g.,* [35, 36]). It is also motivated theoretically, where it is known that Shor's algorithm can be solved with efficient polylogarithmic depth quantum circuits supplemented by classical computation [37]. Can all quantum algorithms be simulated in this way? Understanding this question has long been cited as a major challenge in quantum complexity theory (see *e.g.,* [36, 38]).

Finally, I am interested in developing new error amplification protocols for these restrictive forms of quantum computation. **We recently gave the first method for the space-preserving error amplification of quantum computations [32]**. As a corollary, we showed how to amplify quantum logspace algorithms, as well as "matchgate circuits" to within inverse exponential error. Matchgates are a restricted class of quantum computation introduced by Valiant [39] and relevant to computation with noninteracting fermions [40, 41, 42].

4 The limitations of quantum computation and Hamiltonian complexity

As quantum computers become more scalable, it will increasingly become important to understand the limitations of their capabilities. QMA is the class of problems that can be verified efficiently on a quantum computer, using a polynomial qubit quantum state for a witness. As such it is the quantum generalization of NP, and QMA-hard problems are unlikely to be solved efficiently by quantum computers. Additionally, understanding QMA has important physical relevance, as deciding the ground state energy of a local Hamiltonian to within inverse polynomial precision is a QMA-complete problem [43].

One of the most basic questions about this class involves the power of a quantum vs classical witness. The so-called QMA vs QCMA problem asks how much additional verification power does a quantum witness provide over a classical bitstring? Since it is clear that we don't lose power by considering quantum witnesses our goal is understand if $\mathsf{QMA} \not\subset \mathsf{QCMA}$. Not surprisingly this question has physical motivation: if $\mathsf{QMA} = \mathsf{QCMA}$ there would be an efficient classical description of the ground state of a local Hamiltonian that would allow a quantum computer to estimate its energy. Understanding when there exist efficient classical descriptions of ground states is a major topic of study in condensed matter physics.

We have made the first progress on the QMA vs QCMA question since Aaronson and Kuperberg in 2008 [44, 45]. Aaronson and Kuperberg gave a separation using a "quantum oracle", in which both machines are given quantum query access to a specified unitary transformation. Our result achieves this separation using a significantly more constrained "in-place" oracle.

We define an in-place oracle to be a unitary operator that implements a permutation of standard basis states. Unlike the conventional model of oracle, this operator is not generally equal to its own inverse. This property is crucial in our separation. I am particularly interested in investigating further how this change affects the potential for quantum speedups. For example, is there a generic "Grover-like" search speedup that can be shown in this model?

Another question about QMA concerns the importance of the completeness-soundness gap, which translates in the local Hamiltonian problem to the precision of the estimate of the ground state energy. Using standard amplification techniques, it is known that the power of QMA does not change as long as the gap scales at least inverse polynomially with the input length. **In recent work, we show that so-called PreciseQMA, or QMA with exponentially small gap, exactly equals PSPACE [30, 31]**. This gives a surprising classical characterization of a purely quantum complexity class. The result has many applications in classical and quantum complexity theory. For instance, we use it to show that the problem of deciding if a local Hamiltonian is frustration-free is PSPACE-complete. We hope that this characterization of PreciseQMA will be useful for showing PSPACE upper bounds for other complexity classes. For example, it would be interesting to see if Watrous's celebrated proof of $\mathsf{QIP} \subseteq \mathsf{PSPACE}$ [46] can be simplified by showing $\mathsf{QIP} \subseteq \mathsf{PreciseQMA} = \mathsf{PSPACE}$. Further, can we use our result to find the first nontrivial upper-bound for $\mathsf{QMA}(2)$, the class of problems verifiable with two unentangled quantum witnesses? Better understanding this class has long been a goal of my research (see [47]) with relevance to fundamental questions involving quantum entanglement and classical hardness of approximation results (see *e.g.,* [48, 49, 50]).

5 Quantum cryptography and the obfuscation of quantum functionality

It is clear that the advent of quantum computation will significantly change the foundations of modern cryptography. My goal is both to understand how to protect information against quantum adversaries and separately how to take advantage of the counterintuitive properties of quantum mechanics to achieve new cryptographic functionality impossible to achieve classically.

Some of the most exciting recent work in classical cryptography surrounds the notion of "program obfuscation". An obfuscator is (roughly) a procedure that takes as input the code for some program and outputs another functionally equivalent program whose functionality cannot be determined by looking at its source code.

An obfuscator would certainly be one of the most capable tools in the cryptographer's toolkit. The strongest forms could be used to directly implement nearly any desired cryptographic primitive– ranging from one-way functions and public key encryption to fully homomorphic encryption and secure multiparty computation (see *e.g.,* [51, 52]).

A famous result of Barak et. al., proved that the very strongest definition of obfuscation known as "black-box" obfuscators are impossible [51]. Black-box obfuscation is also arguably the most intuitive notion, demanding that anything an adversary can learn by looking at the code of the obfuscated program could have just as well been learned from black-box access to the program. Recently, exciting candidate constructions of weaker, but still extremely useful forms of classical obfuscation have been proposed, reawakening great interest in this area (see *e.g.,* [53, 54]).

We have taken the first step toward understanding the feasibility of a variety of quantum notions of obfuscation [55]. Quantumly, even achieving the impossibility result for black-box obfuscation do not follow directly from Barak's result, due to the so-called no-cloning theorem, which asserts that it is impossible to create an identical copy of an unknown quantum state [56]. Despite this we are able to prove that many notions of obfuscation are still impossible, even in fully quantum settings. In so doing, we developed new definitions and results on computational security models for encryption of quantum plaintext [55, 57].

However, unlike in the classical setting there is still a notion of quantum black-box obfuscation that *may* be possible: an obfuscator that outputs a quantum state. Indeed, we show that this remaining formulation would still be capable of achieving impressive cryptographic functionality [55]. Can we construct quantum obfuscators using ideas from recent results in quantum tomography that show how to achieve quantum functionality using several copies of a quantum state (see *e.g.,* [58, 59])? Classically, candidate constructions have been shown for different, less-intuitive notions of obfuscation, that nonetheless have extremely powerful cryptographic applications (see *e.g.,* [53, 54]). Are the hardness assumptions required by these constructions secure against quantum adversaries? Can we find suitable analogues for the obfuscation of quantum functionality? These are questions that will certainly be important in understanding cryptography in the not-too-distant future.

References

[1] P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings of the 35th IEEE Annual Symposium on Foundations of Computer Science (FOCS)*, pp. 124–134, 1994.

[2] E. Bernstein and U. V. Vazirani, "Quantum complexity theory," *SIAM J. Comput.*, vol. 26, no. 5, pp. 1411–1473, 1997.

[3] S. Aaronson, "BQP and the polynomial hierarchy," in *STOC*, pp. 141–150, 2010.

[4] S. Aaronson, "A counterexample to the Generalized Linial-Nisan conjecture," *ECCC Report 109*, 2010.

[5] J. Watrous, "Succinct quantum proofs for properties of finite groups," in *41st Annual Symposium on Foundations of Computer Science, FOCS 2000, 12-14 November 2000, Redondo Beach, California, USA*, pp. 537–546, 2000.

[6] B. Fefferman and C. Umans, "Pseudorandom generators and the BQP vs. PH problem," *Featured Talk, QIP 2011*, 2010. arXiv:1005.1407.

[7] B. Fefferman, R. Shaltiel, C. Umans, and E. Viola, "On beating the hybrid argument," *Theory of Computing*, vol. 9, pp. 809–843, 2013.

[8] N. Nisan and A. Wigderson, "Hardness vs randomness," *J. Comput. Syst. Sci.*, vol. 49, no. 2, pp. 149–167, 1994.

[9] B. M. Terhal and D. P. DiVincenzo, "Adaptive quantum computation, constant-depth quantum circuits and Arthur-Merlin games," *Quantum Information and Computation*, vol. 4, no. 2, pp. 134–145, 2004.

[10] M. J. Bremner, R. Jozsa, and D. J. Shepherd, "Classical simulation of commuting quantum computations implies collapse of the Polynomial Hierarchy," *Proceedings of the Royal Society A*, vol. 467, no. 2126, pp. 459–472, 2010. arXiv:1005.1407.

[11] S. Aaronson and A. Arkhipov, "The computational complexity of linear optics," in *STOC '11: Proceedings of the 43rd annual ACM Symposium on Theory of Computing*, pp. 333–342, 2011. arXiv:1011.3245.

[12] M. A. Broome, A. Fedrizzi, S. Rahimi-Keshari, J. Dove, S. Aaronson, T. C. Ralph, and A. G. White, "Photonic boson sampling in a tunable circuit," *Science*, vol. 339, p. 6121, 2013.

[13] A. Crespi, R. Osellame, R. Ramponi, D. J. Brod, E. F. Galvao, N. Spagnolo, C. Vitelli, E. Maiorino, P. Mataloni, and F. Sciarrino, "Integrated multimode interferometers with arbitrary designs for photonic boson sampling," *Nature Photonics*, vol. 7, pp. 545–549, 2013.

[14] T. C. Ralph, “Quantum computation: Boson sampling on a chip,” *Nature Photonics*, vol. 7, pp. 514–515, 2013.

[15] J. B. Spring, B. J. Metcalf, P. C. Humphreys, W. S. Kolthammer, X.-M. Jin, M. Barbieri, A. Datta, N. Thomas-Pter, N. K. Langford, D. Kundys, J. C. Gates, B. J. Smith, P. G. R. Smith, and I. A. Walmsley, “Boson sampling on a photonic chip,” *Science*, vol. 339, pp. 798–801, 2013.

[16] M. Tillman, B. Dakic, R. Heilmann, S. Nolte, A. Szameit, and P. Walther, “Experimental boson sampling,” *Nature Photonics*, vol. 7, pp. 540–544, 2013.

[17] M. Bentivegna, N. Spagnolo, C. Vitelli, F. Flamini, N. Viggianiello, L. Latmiral, P. Mataloni, D. J. Brod, E. F. Galvão, A. Crespi, R. Ramponi, R. Osellame, and F. Sciarrino, “Experimental scattershot boson sampling,” *Science Advances*, vol. 1, no. 3, p. e1400255, 2015. arXiv:1505.03708.

[18] K. R. Motes, J. P. Dowling, A. Gilchrist, and P. P. Rohde, “Implementing scalable boson sampling with time-bin encoding: analysis of loss, mode mismatch, and time jitter,” *Physical Review A*, vol. 92, p. 052319, 2015. arXiv:1507.07185.

[19] S. Aaronson and D. J. Brod, “BosonSampling with lost photons,” *Physical Review A*, vol. 93, p. 012335, 2016. arXiv:1510.05245.

[20] C. Shen, Z. Zhang, and L.-M. Duan, “Scalable implementation of boson sampling with trapped ions,” *Physical Review Letters*, vol. 112, p. 050504, 2014.

[21] B. Peropadre, A. Aspuru-Guzik, and J. J. Garcia-Ripoll, “Spin models and boson sampling,” *arXiv:1509.02703*, 2015.

[22] B. Fefferman and C. Umans, “On the power of quantum Fourier sampling,” in *Proceedings of Theory of Quantum Computation, Communication and Cryptography*, 2016. arXiv:1507.05592.

[23] B. Fefferman, M. Foss-Feig, and A. Gorshkov, “Exact sampling hardness of ising spin models,” 2016.

[24] A. Bouland, L. Mancinska, and X. Zhang, “Complexity classification of two-qubit commuting Hamiltonians,” in *CCC ’16: Proceedings of the 31st Conference on Computational Complexity*, pp. 28:1–28:33, 2016. arXiv:1602.04145.

[25] A. Ta-Shma, “Inverting well conditioned matrices in quantum logspace,” in *Symposium on Theory of Computing Conference, STOC’13, Palo Alto, CA, USA, June 1-4, 2013* (D. Boneh, T. Roughgarden, and J. Feigenbaum, eds.), pp. 881–890, ACM, 2013.

[26] J. Watrous, “On the complexity of simulating space-bounded quantum computations,” *Computational Complexity*, vol. 12, no. 1-2, pp. 48–84, 2003.

[27] S. Lloyd, M. Mohseni, and P. Rebentrost, “Quantum principal component analysis,” *Nature Physics*, vol. 10, pp. 631–633, 2014.

[28] B. D. Clader, B. C. Jacobs, and C. R. Sprouse, “Preconditioned quantum linear system algorithm,” *Physical Review Letters*, vol. 110, p. 250504, 2013. arXiv:1301.2340.

[29] S. Aaronson, “Quantum machine learning algorithms: read the fine print,” *Nature Physics*, vol. 11, pp. 291–293, 2015.

[30] B. Fefferman and C. Y. Lin, "Quantum Merlin Arthur with Exponentially Small Gap," *CoRR*, vol. abs/1601.01975, 2016.

[31] B. Fefferman and C. Y. Lin, "A Complete Characterization of Unitary Quantum Space," *Accepted Talk, QIP 2017.* ArXiv:1604.01384.

[32] B. Fefferman, H. Kobayashi, C. Y. Lin, T. Morimae, and H. Nishimura, "Space-efficient error reduction for unitary quantum computations," *In Proceedings, ICALP*, 2016. arXiv:1604.08192.

[33] A. W. Harrow, A. Hassidim, and S. Lloyd, "Quantum algorithm for linear systems of equations," *Phys. Rev. Lett.*, vol. 103, p. 150502, Oct 2009.

[34] A. Broadbent and E. Kashefi, "Parallelizing quantum circuits," *Theor. Comput. Sci.*, vol. 410, no. 26, pp. 2489–2510, 2009.

[35] C. Moore and M. Nilsson, "Parallel quantum computation and quantum codes. quant-ph/9808027," 1998.

[36] R. Jozsa, "An introduction to measurement based quantum computation," Jul 2005.

[37] R. Cleve and J. Watrous, "Fast parallel circuits for the quantum fourier transform," in *41st Annual Symposium on Foundations of Computer Science, FOCS 2000, 12-14 November 2000, Redondo Beach, California, USA*, pp. 526–536, 2000.

[38] S. Aaronson, "Ten Semi-Grand Challenges for Quantum Computing Theory," 2005.

[39] L. G. Valiant, "Quantum circuits that can be simulated classically in polynomial time," *SIAM Journal on Computing*, vol. 31, no. 4, pp. 1229–1254, 2002.

[40] B. M. Terhal and D. P. DiVincenzo, "Classical simulation of noninteracting-fermion quantum circuits," *CoRR*, 2001. arXiv:quant-ph/0108010.

[41] R. Jozsa, B. Kraus, A. Miyake, and J. Watrous, "Matchgate and space-bounded quantum computations are equivalent," *Proceedings of the Royal Society A*, vol. 466, no. 2115, pp. 809–830, 2010.

[42] R. Jozsa and A. Miyake, "Matchgates and classical simulation of quantum circuits," *Proceedings of the Royal Society A*, vol. 464, no. 2100, pp. 3089–3106, 2008.

[43] A. Kitaev, A. Shen, and M. Vyalyi, *Quantum and Classical Computation.* AMS, 2002.

[44] S. Aaronson and G. Kuperberg, "Quantum versus classical proofs and advice," *Theory of Computing*, vol. 3, no. 1, pp. 129–157, 2007.

[45] B. Fefferman and S. Kimmel, "Quantum vs classical proofs and subset verification," *CoRR*, vol. abs/1510.06750, 2015.

[46] R. Jain, Z. Ji, S. Upadhyay, and J. Watrous, "QIP = PSPACE," *J. ACM*, vol. 58, no. 6, p. 30, 2011.

[47] S. Aaronson, S. Beigi, A. Drucker, B. Fefferman, and P. W. Shor, "The power of unentanglement," *Theory of Computing*, vol. 5, no. 1, pp. 1–42, 2009.

[48] F. G. S. L. Brandão, M. Christandl, and J. Yard, "A quasipolynomial-time algorithm for the quantum separability problem," in *Proceedings of the 43rd ACM Symposium on Theory of Computing, STOC 2011, San Jose, CA, USA, 6-8 June 2011* (L. Fortnow and S. P. Vadhan, eds.), pp. 343–352, ACM, 2011.

[49] A. W. Harrow and A. Montanaro, “An Efficient Test for Product States with Applications to Quantum Merlin-Arthur Games,” in *51th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2010, October 23-26, 2010, Las Vegas, Nevada, USA*, pp. 633–642, IEEE Computer Society, 2010.

[50] B. Barak, F. G. S. L. Brandão, A. W. Harrow, J. A. Kelner, D. Steurer, and Y. Zhou, “Hypercontractivity, sum-of-squares proofs, and their applications,” in *Proceedings of the 44th Symposium on Theory of Computing Conference, STOC 2012, New York, NY, USA, May 19 - 22, 2012* (H. J. Karloff and T. Pitassi, eds.), pp. 307–326, ACM, 2012.

[51] B. Barak, O. Goldreich, R. Impagliazzo, S. Rudich, A. Sahai, S. P. Vadhan, and K. Yang, “On the (im)possibility of obfuscating programs,” *J. ACM*, vol. 59, no. 2, p. 6, 2012.

[52] B. Barak, “Hopes, fears, and software obfuscation,” *Commun. ACM*, vol. 59, no. 3, pp. 88–96, 2016.

[53] S. Garg, C. Gentry, S. Halevi, M. Raykova, A. Sahai, and B. Waters, “Candidate indistinguishability obfuscation and functional encryption for all circuits,” *SIAM J. Comput.*, vol. 45, no. 3, pp. 882–929, 2016.

[54] A. Sahai and B. Waters, “How to use indistinguishability obfuscation: deniable encryption, and more,” in *Symposium on Theory of Computing, STOC 2014, New York, NY, USA, May 31 - June 03, 2014* (D. B. Shmoys, ed.), pp. 475–484, ACM, 2014.

[55] G. Alagic and B. Fefferman, “On quantum obfuscation,” *Accepted talk, QCrypt 2016.* ArXiv:1602.01771.

[56] W. K. Wootters and W. H. Zurek, “A single quantum cannot be cloned,” *Nature*, vol. 299, pp. 802–803, 10 1982.

[57] G. Alagic, A. Broadbent, B. Fefferman, T. Gagliardoni, C. Schaffner, and M. S. Jules, “Computational security of quantum encryption,” *Accepted talk, QCrypt 2016.*

[58] S. Lloyd, M. Mohseni, and P. Rebentrost, “Quantum principal component analysis,” *Nat Phys*, vol. 10, pp. 631–633, 09 2014.

[59] S. Kimmel, C. Y.-Y. Lin, G. H. Low, M. Ozols, and T. J. Yoder, “Hamiltonian simulation with optimal sample complexity,” *arXiv preprint arXiv:1608.00281*, 2016.