Indian Institute of Management Calcutta

Working Paper Series

WPS No. 789
November 2016

Data Analytics in Quantum Paradigm – An Introduction

Arpita Maitra
Research Assistant
Indian Institute of Management Calcutta, D. H. Road, Joka, P.O. Kolkata 700 104
Email: arpita76b@gmail.com

Subhamoy Maitra
Professor
Indian Statistical Institute, 203 Barrackpore Trunk Road, Kolkata - 700108
Email: subho@isical.ac.in

Asim K. Pal
Professor
Indian Institute of Management Calcutta
D. H. Road, Joka, P.O. Kolkata 700 104
http://facultylive.iimcal.ac.in/workingpapers

Data Analytics in Quantum Paradigm – An Introduction

Arpita Maitra , Subhamoy Maitra[†] and Asim K. Pal[‡]

Abstract In this introductory material, we will discuss basics of quantum paradigm and how the developments in that area may provide useful pointers in the domain of data analytics. We will discuss about the power of quantum computation with respect to the classical one and try to present the implications of arrival of several quantum technologies in practice. The prime concerns in data analytics are fast computation, fast communication and security of data. Among these issues, the main focus is naturally on the computation and then the rest of the issues follow. The objective of getting better efficiency can be attained by discrete algorithms with improved (lesser) time complexity and it is now proven that there are quantum algorithms that are indeed much faster than their classical counterparts. However, in all the domains of computation, such improvements may not be available and also fabricating a commercial quantum computer is still elusive. We will try to briefly

Arpita Maitra
Indian Institute of Management Calcutta, e-mail: arpita76b@gmail.com

Subhamoy Maitra
Indian Statistical Institute, Kolkata e-mail: subho@isical.ac.in

Asim K. Pal
Indian Institute of Management Calcutta, e-mail: asim@iimcal.ac.in

This author is supported by the project "Information Security and Quantum Cryptography: Study of Secure Multi-Party Computation in Quantum Domain and Applications" at IIM Calcutta.

[†] This author is supported by the project "Cryptography & Cryptanalysis: How far can we bridge the gap between Classical and Quantum Paradigm", awarded by the Scientific Research Council of the Department of Atomic Energy (DAE-SRC), the Board of Research in Nuclear Sciences (BRNS).

[‡] This author is supported by the projects "Sentiment analysis: An approach with data mining, computational intelligence and longitudinal analysis with Applications to finance and marketing" as well as "Information Security and Quantum Cryptography: Study of Secure Multi-Party Computation in Quantum Domain and Applications" at IIM Calcutta.

lutions in the quantum domain. Consider the example of a share market. There we require huge computation in short time, need to communicate those data quickly among different parties and at the same time the data security has to be considered with priority. While the data communication and security issues may be handled as a part where much competition might not be involved, each of the companies will be interested to have a better forecast than the other. Towards a better forecast, which is the main purpose of data analytics, one requires to have huge statistical calculations, which finally boils down to arithmetic, algebraic, combinatorial and symbolic computations. Thus, the main question here is whether we can have better computational facilities in quantum paradigm. This is the focus of this material. At the same time, we also touch a few issues in communication and security domain that are relevant in data analytics and where the quantum paradigm has efficient tools to offer.

Before proceeding further, let us present brief introductory materials. For detailed technical understanding, one may refer to [29].

1.1 Basics of a qubit and the algebra

As a bit (0 or 1) is the basic element of a classical computer, the quantum bit (called the qubit) is the fundamental element in the quantum paradigm, whose physical counterpart is a photon. A qubit is represented as

$$a|0\rangle + b|1\rangle;$$

where $a; b \in \mathbb{C}$ (i.e., complex numbers), and $|a|^2 + |b|^2 = 1$. If one measures the qubit in $\{|0\rangle; |1\rangle\}$ basis, then $|0\rangle$ is observed with probability $|a|^2$, and $|1\rangle$ with $|b|^2$. The original state gets destroyed after the observation and collapse to the observed state.

That is, the qubits $|0\rangle; |1\rangle$ are the quantum counterparts of the classical bits $0; 1$. The qubit $|0\rangle$ can be represented as $\begin{matrix}1\\0\end{matrix}$ and $|1\rangle$ can be represented as $\begin{matrix}0\\1\end{matrix}$. The superposition of $|0\rangle; |1\rangle$, i.e., $a|0\rangle + b|1\rangle$ can be written as $a\begin{matrix}1\\0\end{matrix} + b\begin{matrix}0\\1\end{matrix} = \begin{matrix}a\\b\end{matrix}$, where $a; b \in \mathbb{C}$, $|a|^2 + |b|^2 = 1$.

Based on this definition, one may theoretically pack infinite amount of information in a single qubit. However, it is not clear how to extract such information. Further in actual implementation of quantum circuits, it might not be possible to perfectly create a qubit for any $a; b$. Nevertheless, it is clear that a single qubit may contain huge information compared to a bit.

The basic algebra relating to more than one qubits can be interpreted as tensor products. Thus, consider tensor product of two qubits as

$$(a_1 j0i + b_1 j1i) \quad (a_2 j0i + b_2 j1i) = \begin{matrix} a_1 & a_2 \\ b_1 & b_2 \end{matrix} = \begin{matrix} a_1 & a_2 \\ b_1 & a_2 \\ a_1 & b_2 \\ b_1 & b_2 \end{matrix} = \begin{matrix} a_1 a_2 \\ b_1 a_2 \\ a_1 b_2 \\ b_1 b_2 \end{matrix}$$

$$= a_1 a_2 \begin{matrix} 1 \\ 0 \\ 0 \\ 0 \end{matrix} + a_1 b_2 \begin{matrix} 0 \\ 1 \\ 0 \\ 0 \end{matrix} + b_1 a_2 \begin{matrix} 0 \\ 0 \\ 1 \\ 0 \end{matrix} + b_1 b_2 \begin{matrix} 0 \\ 0 \\ 0 \\ 1 \end{matrix}$$

$= a_1 a_2 j00i + a_1 b_2 j01i + b_1 a_2 j10i + b_1 b_2 j11i$. That is,
$(a_1 j0i + b_1 j1i) \quad (a_2 j0i + b_2 j1i) = a_1 a_2 j00i + a_1$

The 2-input 2-output quantum gates can be seen as 4×4 unitary matrices. An example is the CNOT gate which works as follows: $|00\rangle \rightarrow |00\rangle$, $|01\rangle \rightarrow |01\rangle$, $|10\rangle \rightarrow |11\rangle$, $|11\rangle \rightarrow |10\rangle$. The related matrix is $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$.

As an application of these gates, let us describe the circuit in Figure 1 to create certain entangled states as follows: $|b_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$, $|b_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$, $|b_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$, and $|b_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$.

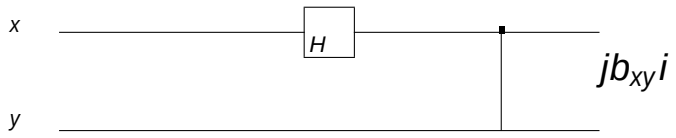

Fig. 1 Quantum circuit for creating entangled state

1.3 No cloning

While it is very easy to copy an unknown classical bit (i.e., either 0 or 1), it is now well known that it is not possible to copy an unknown qubit. This result is known as the "no cloning theorem" and was initially noted in [13, 43]. It has a huge implicationicating entangled state a huge

From the inner product: $hsjhy jU^{\dagger}Ujf ijsi = hy jhy jjf ijf i$. This implies $hy jf i = (hy jf i)^2$.

Note that $x = x^2$ has only two solutions: $x = 0$ and $x = 1$. Thus we get either $jy i = jf i$ or inner product of them equals to zero, i.e., $jy i$ and $jf i$ are orthogonal to each other. This implies that a cloning device can only clone orthogonal states. Therefore a general quantum cloning device is impossible. For example, given that the unknown state is one of $j0i$, $\frac{j0i+j1i}{\sqrt{2}}$, two nonorthogonal states, it is not possible to clone the state without knowing which one it is.

This provides certain advantages as well as disadvantages. The advantages are in the domain of quantum cryptography, where by the laws of physics copying an unknown qubit is not possible. However, in terms of copying or saving unknown quantum data, this is actually a potential disadvantage. At the same time, it should be clearly explained that given a known quantum state, it is always possible to copy it. This is because, for a known quantum state, we know how to create it deterministically and thus it is possible to reproduce it with the same circuit.

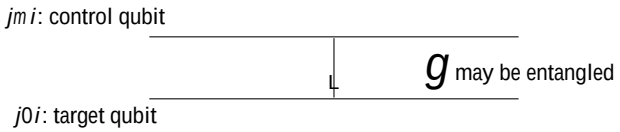

Fig. 2

2 A brief overview of advantages in Quantum Paradigm

Next we like to briefly mention a couple of areas where the frameworks based on quantum physics provide advantageous situations over the classical domain. We will consider one example each in the domain of communication as well as computation.

2.1 Teleportation

Teleportation is one of the important ideas that shows the strength of quantum model

The importance of this technique in data analytics is that if two different places may share entangled particles, then it is possible to send a huge amount of information (in fact theoretically infinite) by just communicating two classical bits. Again, one important issue to be noted is that, even if we manage to trasport a qubit, in case it is unknown, it might not be possible to extract the relevant information from that.

2.2 Deutsch-Jozsa Algorithm

Deutsch-Jozsa algorithm [12] is possibly the first clear example that demonstrates quantum parallelism over the standard classical model. Take a Boolean function $f : f0;1g^n \; ! \; f0;1g$. A function f is constant if $f(x) = c$ for all $x \; 2 \; f0;1g^n$, $c \; 2 \; f0;1g$. Further f is called balanced if $f(x) = 0$ for $2^{n \; 1}$ inputs and $f(x) = 1$ for the rest of $2^{n \; 1}$ inputs. Given the function f as a black box, which is either constant or balanced, we need an algorithm, that can answer which one this is. It is clear that a classical algorithm needs to check the function for at least $2^{n \; 1} + 1$ inputs in worst case to come to a decision. Quantum algorithm can solve this with only one input. Note that given a classical circuit f, there is a quantum circuit of comparable efficiency which computes the transformation U_f that takes input like $jx;yi$ and produces output like $jx;y \quad f(x)i$.

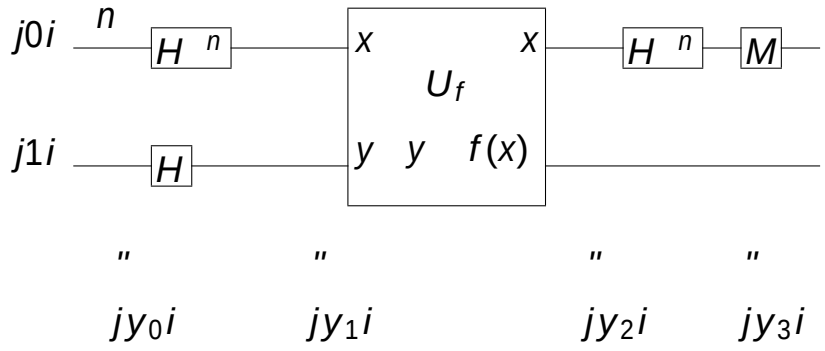

Fig. 4 Quantum circuit to implement Deutsch-Jozsa Algorithm

The step by step operations of the technique can be described as follows.

$$jy_0i = j0i \; ^n j1i$$

$$jy_1i = \text{å}_{x2f0;1g^n} \frac{jxi}{\sqrt{2^n}} \; \text{h} \; \frac{j0i_p j1i}{\sqrt{2}} \; \text{i}$$

$$jy_2i = \text{å}_{x2f0;1g^n} \frac{(\;1)^{f(x)}jxi}{\sqrt{2^n}} \; \text{h} \; \frac{j0i_p j1i}{\sqrt{2}} \; \text{i}$$

$$jy_3i = \text{å}_{z2f0;1g^n} \text{å}_{x2f0;1g^n} \frac{(\;1)^{x \; z \; f(x)}jzi}{2^n} \; \text{h} \; \frac{j0i_p j1i}{\sqrt{2}} \; \text{i}$$

Measurement: all zero state implies that the function is constant, otherwise it is balanced.

The importance of explaining this algorithm in the context of data analytics is that, it is often important to distinguish between two objects very efficiently. The example of Deutsch-Jozsa algorithm [12] demonstrates that it is significantly efficient compared to the classical domain.

At this point we like to present two important aspects of Deutsch-Jozsa algorithm [12] in terms of data analytics and machine learning. First of all, one must note that we can obtain the equal superposition of all 2^n many n-bit states just by using n many Hadamard gates. For this, note the first part of jy_1i which is $\sum_{x \in \{0,1\}^n} \frac{jxi}{\sqrt{2^n}}$. This provides an exponential advantage in quantum domain as in the classical domain we cannot access all the 2^n many n-bit patterns efficiently. The second point is related to machine learning. As we have discussed, we may have the circuit of f available as a black-box and we like to learn several properties of the function efficiently. In this direction, Walsh transform is an important tool. What we obtain as the output of the Deutsch-Jozsa algorithm just before measurement is jy_3i and the first part of this is $\sum_{z \in \{0,1\}^n} \sum_{x \in \{0,1\}^n} \frac{(-1)^{x \cdot z \oplus f(x)} jzi}{2^n}$. Note that, the Walsh spectrum of the Boolean function f at a point z is defined as $W_f(z) = \sum_{x \in \{0,1\}^n} (-1)^{x \cdot z \oplus f(x)}$. That is, $\sum_{z \in \{0,1\}^n} \sum_{x \in \{0,1\}^n} \frac{(-1)^{x \cdot z \oplus f(x)} jzi}{2^n} = \sum_{z \in \{0,1\}^n} \frac{W_f(z)}{2^n} jzi$. This means that using such an algorithm, we can efficiently obtain a transform domain spectrum of the function, which is not achievable in classical domain.

Testing severales3ting

Int397-332(m97-29(th96 -2teral)-312lz97-2rea2lz97-fTf 497-impoar,)-3597-3n-3597-Tfe675ry(th96 tal)-312lz97-[6],2lz97-50(achiz97-2re-3597-3n-285

The main challenge in cryptology in early seventies was how to decide on a secret information between two parties over a public channel. The solution to this has been

Till date, there is no efficient algorithm to solve DLP or RSA in classical domain.

If only a single basis is used, then the attacker can measure in that basis to obtain the information and reproduce.
Thus Alice needs to encode randomly with more than one bases.
Bob will also measure in random basis.
Basis will match in a proportion of cases and from that the secret key will be prepared.

This is the brief idea to obtain a secret key between two parties over an insecure public channel using the BB84 [5] protocol. After obtaining the secret key, one may use a symmetric key cryptosystem (for example, a stream cipher or a block cipher, see [38] for details) for further communication in encrypted mode. One may refer to [21] for state of the art results of quantum cryptanalysis on symmetric ciphers, though it is still not as havoc as it had been on classical public key schemes.

3.2 Secure Multi-Party Computation

Let us now consider another important aspect of cryptology that might be relevant in data analytics. Take the example of an Automated Teller Machine (ATM) for money transaction. This is a classic example of secure two or multi-party computation. Due to such transactions and several other application domains which are related to secure data handling, Secure Multi-Party Computation (SMC) has become a very important research topic in data intensive areas. In a standard model of SMC, n number of parties wish to compute a function $f(x_1, x_2, \ldots, x_n)$ of their respective inputs $x_1, x_2, \ldots, x_n$, keeping the inputs secret from each other. Such computations have wide applications in online auction, negotiation, electronic voting etc. Yao's millionaire's problem [44] is considered as one of the initial attempts in the domain of SMC. Later, this has been studied extensively in classical domain (see [18] and the references therein). The security of classical SMC usually comes from some computational assumptions such as hardness of factorization of a large number.

In quantum domain, Lo [24] showed the impossibility for secure computation in certain two-party scenario. For example, "one out of two parties secure computation" means that only one out of two parties is allowed to know the output. As a corollary to this result [24], it had been shown that one out of two oblivious transfer is impossible in quantum paradigm. It has been claimed in [22] that given an implementation of oblivious transfer, it is possible to securely evaluate any polynomial time computable function without any additional primitive in classical domain. However, it seems that such a secure two party computation might not work in quantum domain. Hence, in case of two-party quantum computation, some additional assumptions, such as the semi-honest third party etc., have been introduced to obtain the secure private comparison [40].

In [45], Yao had shown that any secure quantum bit commitment scheme can be used to implement secure quantum oblivious transfer. However, Mayers [27] and Lo et al [25] independently proved the insecurity of quantum bit commitment. Very recently some relativistic protocols [26] have been proposed in the domain of quan-

tum SMC. Unfortunately, these techniques are still not very promising for practical implementations. Thus, considering quantum adversaries, it might not be possible to achieve SMC and in turn collaborative multi-party computation in distributed environments without compromising the security.

4 Data Analytics: A Critical View of Quantum Paradigm

Given the background of certain developments in quantum paradigm over the classical world, now let us get into some specific issues of data analytics. The first point is, if we consider use of one qubit just as storing one bit of data, then that would be a significant loss in terms of exploiting the much larger (theoretically infinite) space of a qubit. On the other hand, for analysis of classical data, we may require to consider new implementation of data storage that might add additional overhead as data need to be presented in quantum platform. For example, consider the Deutsch-Jozsa [12] algorithm. To apply this algorithm, we cannot use an n-input 1-output Boolean function, but we require a form where the same function can be realized as a function with equal number of input and output bits. Further the same circuit must be implemented with quantum circuits so that the superposition of qubits can be handled. These are the overheads that need to be considered.

Next let us come to the issue of structured and unstructured data. In classical domain, if a data set with N elements are not sorted, then in worst case, we require $O(N)$ search complexity to find a specific data. In quantum domain, the seminal Grover's algorithm [17] shows that this is possible in only $O(\sqrt{N})$ effort. For a huge unsorted data set, this is indeed a significant gain. However, in any efficient database, the individual data elements are stored in a well-structured manner so that one can identify a specific record in $O(\log N)$ time. This is exponentially small in comparison with both $O(N)$ as well as $O(\sqrt{N})$ and thus, in such a scenario, quantum computers may not be of significant advantage.

4.1 Related quantum algorithms

To achieve any kind of data analysis, we require several small primitives. Let us first consider finding minimum or maximum from an unsorted list. Similar ideas as in [17] can be applied to obtain minimum or maximum value from an unsorted list of size N in $O(\sqrt{N})$ time as explained in [15] and [2] respectively. The work [20] considers in detail quantum searching in ordered list and sorting. However, in such a scenario where ordered lists are maintained, quantum algorithms do not provide

algorithms heavily use results related to quantum walks [39]. In a related direction, solution of a system of linear equations had naturally received serious attention in quantum domain and there are interesting speed-up in several cases. Further these results [19] have applications towards solving linear differential equations, least square techniques and in general, in the domain of machine learning. One may refer to [32] for a detailed description of quantum algorithms and then compare their complexities with the classical counterparts.

While there are certain improvements in specific areas, the situation is not always hopeful and a nice reference in this regard is [1], where Aaronson says

> "Having spent half my life in quantum computing research, I still find it miraculous that the laws of quantum physics let us solve any classical problems exponentially faster than today's computers seem able to solve them. So maybe it shouldn't surprise us that, in machine learning like anywhere else, Nature will still make us work for those speedups."

One may also have a look at [8, 23] for very recent state of the art discussions on quantum supremacy. While most of the explanations do not provide a great recommendation towards advantages of quantum machine learning, for some initial understanding of this area from a positive viewpoint, one may refer to [42].

4.2 Database

The next relevant question is if we have significant development in the area of quantum database. In this direction there are some initial concept papers such as [36]. This work presents a novel database abstraction that allows to defer the finalization of choices in transactions until an entity forces the choices by observation in quantum terminology. Following the quantum mechanical idea, here a transaction is in a quantum state, i.e., it could be one of many possible states or might be a superposition. This is naturally undecided and unknown until observed by some kind of measurement. Such an abstraction enables late binding of values read from the database. The authors claimed that this helps in obtaining more transactions to succeed in a situation with high contention. This scenario might be useful for applications where the transactions compete for physical resources represented by data items in the database, such as booking seats in an airline or buying shares. However, these are more at the conceptual level, where actual implementation related details can not be exactly estimated.

Let us now look at what happens when we are interested in a series of computations which are possibly the most occurring phenomenon in practice. Consider two scenarios, one from a static data set (structured) and another from a dynamic data set where arbitrary search, addition, modification and alteration are allowed. In static case, the database is generally maintained in such a manner so that the search efforts are always logarithmic. Now consider a little more complex scenario, where the database grows or shrinks arbitrarily and the search as well as other write operations are allowed in arbitrary sequence. Even in case of such dynamic updations,

we always try to maintain some well known balanced tree structures. Hence, in both the scenarios, we do not have any clear advantage in quantum domain.

4.3 Text Mining

Text mining is an integral part of data analytics given the popularity of social media.

chains are discussed from a different information-theoretic viewpoint and it is not very clear how long it will take to connect ideas from machine learning domain and the paradigm of quantum information to obtain meaningful commercial results.

5 Conclusion: Google, PageRank and Quantum Advantage

In this review, we have taken an approach to present certain introductory issues in quantum paradigm and then explained how they relate to basics of data analytics. We described several aspects in the domain of computation, communication and security and pointed out why the computational part should receive prime attention. In the quantum computational model, we have enumerated several significant improvements over the classical counterpart, but the two main concerns that remain are as follows.

Can we fabricate a commercially viable quantum computer?
(Even if we have a quantum computer) Can we have significant improvements in computational complexity for algorithms related to data analytics?

Let us now conclude with a very practical and well known problem in the domain of data analytics that received a significant attention. This should help the reader to form his/her own opinion regarding the impact of quantum computation on a significant problem. The problem is related to PageRank. PageRank is an algorithm used by Google Search to rank the websites through their search engine results. It is a method of quantifying the importance of the web pages, i.e., PageRank may be viewed as a metric proposed by Google's owners Larry Page and Sergey Brin. According to Google:

References

1. S. Aaronson. Quantum machine learning algorithms: read the fine print preprint, 2015. Available at http://www.scottaaronson.com/papers/qml.pdf
2. A. Ahuja and S. Kapoor. A Quantum Algorithm for finding the Maximum, 1999. Available at https://arxiv.org/abs/quant-ph/9911082
3. C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, W. K. Wootters. Teleporting an Unknown Quantum State via Dual Classical and EinsteinPodolskyRosen Channels. Phys. Rev. Lett. 70, 1895-1899 (1993).
4. C. H. Bennett and G. Brassard. Quantum cryptography and its application to provably secure key expansion, public-key distribution, and coin-tossing. In Proceedings of IEEE International Symposium on Information Theory, St-Jovite, Canada, page 91, September 1983.
5. C. H. Bennett and G. Brassard. Quantum Cryptography: Public key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 175–179, IEEE, New York (1984)
6. E. Bernstein and U. Vazirani. Quantum complexity theory. Proceedings of the 25th Annual ACM Symposium on Theory of Computing, (ACM Press, New York, 1993), pp. 11–20.
7. D. M. Blei, A. Y. Ng and M. I. Jordan. Latent Dirichlet Allocation. Journal of Machine Learning Research, 3, 993–1022, (2003)
8. S. Boixo, S. V. Isakov, V. N. Smelyanskiy, R. Babbush, N. Ding, Z. Jiang, J. M. Martinis, H. Neven. Characterizing Quantum Supremacy in Near-Term Devices. https://arxiv.org/abs/1608.00263, August 3, 2016
9. G. Brassard. Brief History of Quantum Cryptography: A Personal Perspective. Proceedings of IEEE Information Theory Workshop on Theory and Practice in Information Theoretic Security, Awaji Island, Japan, October 2005, pp. 19 – 23. [quant-ph/0604072]
10. H. Buhrman and R. Spalek. Quantum verification of matrix products. In Proceedings of the 17th ACM-SIAM Symposium on Discrete Algorithms, pages 880–889, 2006. [arXiv:quant-ph/0409035]
11. N. Datta and M. M. Wilde. Quantum Markov chains, sufficiency of quantum channels, and Renyi information measures. Journal of Physics A vol. 48, no. 50, page 505301, November 2015. Available at https://arxiv.org/abs/1501.05636
12. D. Deutsch and R. Jozsa. Rapid solution of problems by quantum computation. Proceedings of Royal Society of London, A439:553–558 (1992).
13. D. Dieks. Communication by EPR devices. Physics Letters A, vol. 92(6) (1982), pp. 271-272.
14. W. Diffie and M. E. Hellman. New Directions in Cryptography. IEEE Transactions on Information Theory, pages 644–654, vol. 22, 1976.
15. C. Durr and P. Hoyer. A Quantum Algorithm for Finding the Minimum, 1996 Available at https://arxiv.org/abs/quant-ph/9607014
16. T. L. Griffiths and M. Steyvers. Finding scientific topics. Proceedings of the National Academy of Sciences of the United States of America (PNAS), 5228–5235, vol. 101, suppl. 1 April 6, 2004. Available at www.pnas.org/cgi/doi/10.1073/pnas.0307752101
17. L. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of 28th Annual Symposium on the Theory of Computing (STOC)*, May 1996, pages 212–219. Available at http://xxx.lanl.gov/abs/quant-ph/9605043
18. S. D. Gordon, C. Hazay, J. Katz and Y. Lindell. Complete Fairness in Secure Two-Party Computation. Proceedings of the 40-th Annual ACM symposium on Theory of Computing (STOC), 413422, ACM Press, (2008)
19. A. W. Harrow, A. Hassidim, and S. Lloyd. Quantum algorithm for linear systems of equations. Physical review letters, 103(15):150502, 2009. Available at https://arxiv.org/abs/0811.3171
20. P. Hoyer, J. Neerbek and Y. Shi. Quantum complexities of ordered searching, sorting, and element distinctness, 2001. Available at https://arxiv.org/abs/quant-ph/0102078
21.

22. J. Killan. Founding Cryptography on Oblivious Transfer. Proceedings of the 20th Annual ACM Symposium on the Theory of Computation (STOC), (1988).
23. https://rjlipton.wordpress.com/2016/04/22/quantum-supremacy-and-complexity/, April 22, 2016
24. H. -K. Lo. Insecurity of quantum secure computations. Phy. Rev. A 56, 11541162, (1997)
25. H. -K. Lo and H. F. Chau. Is Quantum Bit Commitment Really Possible? Phys. Rev. Lett. 78, 3410 (1997)
26. T. Lunghi, J. Kaniewski, F. Bussieres, R. Houlmann, M. Tomamichel, S. Werner and H. Zbinden. Practical relativistic bit commitment, Phys. Rev. Lett. 115, 030502 (2015)
27. D. Mayers. Unconditionally secure quantum bit commitment is impossible. Phys. Rev. Lett. 78, 3414 (1997)
28. A. Montanaro. Quantum speedup of Monte Carlo methods. Proc. R. Soc. A 471: 20150301, 2015. Available at http://dx.doi.org/10.1098/rspa.2015.0301
29. M. A. Nielsen and I. L. Chuang. Quantum Computation and Quantum Information. Cambridge University Press, 2010.
30. G. D. Paparo and M. A. Martin-Delgado. Google in a Quantum Network. Sci. Rep. 2, 444 (2012) Available at https://arxiv.org/abs/1112.2079
31. Post-quantum Cryptography. http://pqcrypto.org/
32. Quantum Algoritm Zoo. http://math.nist.gov/quantum/zoo/
33. Quantum Key Distribution Equipment. ID Quantique (IDQ). http://www.idquantique.com/
34. Quantum Key Distribution System (Q-Box). MagiQ Technologies Inc. http://www.magiqtech.com
35. R. L. Rivest, A. Shamir and L. Adleman. A Method for Obtaining Digital Signatures and Public Key Cryptosystems. Communications of the ACM, pages 120–126, vol. 21, 1978.
36. S. Roy, L. Kot and C. Koch. Quantum Databases. The 6th Biennial Conference on Innovative Data Systems Research (CIDR), 2013.
37. P. W. Shor. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. Foundations of Computer Science (FOCS) 1994, page 124–134, IEEE Computer Society Press.
38. D. Stinson. *Cryptography Theory and Practice*. Chapman & Hall / CRC, Third Edition, (2005).
39. M. Szegedy. Quantum speed-up of Markov chain based algorithms. In Proceedings of the 45th IEEE Symposium on Foundations of Computer Science, 32–41, 2004.
40. H. Y. Tseng, J. Lin, T. Hwang. New quantum private comparison protocol using EPR pairs. Quantum Information Processing 11, 373–384, (2012).
41. S. Wiesner. Conjugate Coding. Manuscript 1970, subsequently published in SIGACT News 15:1, 78–88, 1983.
42. P. Wittek. Quantum Machine Learning: What Quantum Computing Means to Data Mining. http://peterwittek.com/book.html, 2014
43. W. K. Wootters and W. H. Zurek. A Single Quantum cannot be Cloned. Nature 299 (1982), pp. 802803.
44. A. C. Yao. Protocols for secure computations. 23rd Annual Symposium on Foundations of Computer Science (FOCS), 160164, (1982).
45. A . C. Yao. Security of quantum protocols against coherent measurements, In Proceedings of 26th Annual ACM Symposium on the Theory of Computing (STOC), 67, (1995).