An Investigation into the Ethical Issues in the Applications of a few Quantum Algorithms

Eric Foote

November 2017

Abstract

Quantum computing is manipulating the laws of quantum mechanics for the purposes of examining information. One of the reasons this is useful is cryptography. For example, factoring large integers (finding the prime factorization) and finding the discrete logarithm of a large integer, problems that are really difficult to a classical computer are made more efficient when you run the computation on a quantum computer. This however, poses a ethical issue because the method that RSA encryption is secure is based on classical computers having a hard time finding the prime factorization of large integers and solving the discrete log problem. We will see that Shor's algorithm breaks this. We will also consider some other problems and see the ethical issues in them. We are going to see a common theme throughout and that is quantum computing like classical computing has no special unique ethical issues, its issues lie in how you apply the computer

1 Keywords

Quantum, Quantum Algorithm, Ethical Issues, Quantum Mechanics, Privacy

2 Introduction

Quantum computing manipulates the laws of quantum mechanics to process information. Quantum computers currently would speed up only a select few problems, for example, breaking certain cryptographic algorithms like RSA (Rivest, Shamir, Adleman). However, quantum computers currently have the same algorithmic limitations as a classical computer with respect to most other problems. Quantum computers use qubits instead of bits, the difference being that a qubit is a particle with a quantum state of either spin up which normally corresponds to a 1 or spin down which corresponds to a 0 or a superposition which simultaneously involves spin up and spin down; a few qubits in superposition can store a lot of information and the method that you interact with a quantum computer is you manipulate the numbers stored not the actual qubit itself.We store and

manipulate the data because when you have a n particles in your system you will have n^2 information because of superposition (a quantum system can be occupy multiple states at the same time)[17] and entanglement ("an extremely strong correlation that exists between quantum particles")[17] and if you try to measure this system all you will get is n pieces of information because when you measure a quantum system you disturb the state of the system. Therefore, the challenge of quantum algorithms is to manipulate the n^2 data and extract only the important information. We should look into the ethical issues associated with this kind of computing because as it relates to cryptography because most cryptographic algorithms out there like RSA for example derive their security on factoring large integers and discrete logarithms being in a class of hard problems. Through the remainder of this piece we are first going to briefly look at a rough time line of quantum computing from the beginning to the modern day, we are going to go through RSA encryption because it is a very well known and easy to understand cryptographic algorithm and look at some quantum computing algorithms where I will first give the rough idea about what the algorithm is achieving then run through the process about how it is achieved, trying not to get too technical about the whole process just giving a rough overview of the topic in as close to my own words as possible starting first with Shor's Algorithm then look at an algorithm for solving linear systems of equations then we will explore Grover's search algorithm, then study a verification algorithm and look at an application of it in Quantum Lockers, then look at the Deutsch-Jozsa algorithm, then briefly consider an alternate algorithm for computing discrete logs and factoring RSA integers,look at a quantum set decoding algorithm and finally a quantum algorithm for solving the closest vector problem while we are going through them I will bring up whether or not the author(s) discussed any ethical issues and then touch briefly about my personal take on that specific algorithm's ethical issues then in the discussion section we will bring everything together that we discussed earlier for each individual algorithm and then compare each algorithm's issues and draw some conclusions about the overall issues while also bringing together some of my personal thoughts and feelings about the ethical issues. However, firstly I am going to discuss the personal motivation behind my desire to explore this unknown topic.

3 Motivation

The motivation behind this investigation into the ethical issues in a few applications of quantum algorithms is I really wanted to learn about quantum computing because its the intersection between mathematical physics, quantum mechanics and computer science and there is a lot of probability associated in quantum mechanics so this is really the intersection between all three of my disciplines that I am currently studying those being mathematics, statistics and computer science. Furthermore, this field is a really new and interesting field with many implications some of which we are going to be studying later on in the methods section when we start to look at a few possible algorithms. This

field also really interests me because I want to see how people achieve this manipulation of quantum mechanical principles like entanglement, superposition and teleportation I also wanted to see how our current cryptosystems like RSA, like Diffie-Hellman can be broken because this is not the first time the advent of technology has rendered cryptosystems, like the shift-cipher obsolete. Also I want to bring up as we are getting closer to this technology having more capabilities e.g. IBM's 50 qubit processor [8] the ethical issues that exist currently like privacy concerns, and I also want to explore if authors have already through the years considered them already or if they have not and if they have not I want to try to address them as best I can to do this I am going to not just use as examples the older algorithms like Shors or Grovers but I am also going to use some newer not as famous ones to see if they are being adressed.

4 Background

Quantum computing's roots can be traced back to the 1980's when in 1982 Richard Feynman postulated whether or not quantum mechanics can be simulated on a quantum computer, later, in 1985 David Deutsch proposed the abstract mathematical concept of a quantum Turing machine. While this was going on Bennett and Brassard proposed in 1984 to use Quantum mechanics to send keys for cryptography. In the 1990's Quantum teleportation was proposed and later demonstrated. The basic idea behind teleportation is Alice and Bob start by sharing a pair of entangled (there exist systems of multiple parts which cannot be described only in terms of their constituent parts) qubits, Alice does some manipulation to their piece and the piece they want to send, then Alice sends the measurement result of the piece they wanted to send to Bob and then Bob does some correction to their qubit based on the result given. First, we need to discuss what is called quantum gate arrays or quantum acyclic circuits[16] to do this, consider a system with n components. In the non quantum case a description of this system only needs n bits, however, quantum requires $2^n - 1$ complex numbers or in other words its a point in a 2^n dimension vector space. Since we can describe this as a vector space we can describe this as a basis vector $\langle 1, 0, 0, ... >$ (e.g. 1 is the value of the first bit and 0 is the value of the second bit and so on) for simplicity $\langle x >$ means that x is a pure quantum state. In order to actually perform some computations we need to consider the laws of quantum mechanics which only allow for unitary transformations of state vectors, where a unitary matrix is one whose transpose is equal to its inverse this accomplishes something really cool, basically summing over the probability of all possible outcomes will always return a value of 1. Now that this has finally been built up we can finally talk about quantum acyclic circuits which by definition only allow unitary transformations on a fixed number of bits. The set of 2 bit transformations form the logical building blocks (AND, OR or NOT gates) of quantum circuits, a quantum gate array is a set of quantum gates. This definition of a quantum gate array gives us a particularly useful fact knowing the state of the logical "wires" going out can tell us the state of the going

into the "wires", this means that we can solve any $O(N)$ (where N is some polynomial function) $f(x)$ as long as x stays inside the computer. Before we go consider some algorithms we should step back and take a look at the field of cryptography. By definition cryptography is the study of techniques and systems to protect data and communications from unauthorized interception or tampering[19]. One of the most widely used encryption schemas is RSA (Rivest, Shamir, Adleman, 1977) and in order to recieve messages from Alice, Bob needs to choose two distinct prime numbers p and q and multiply them together to get n and also compute something called the Euler Phi-Function which since p and q were chosen to be prime numbers is $(p-1)(q-1)$[12] then Bob picks an element e from the sub group of integers from $1 -> \phi(n)-1$ which are relatively prime ($gcd(\phi(n), e) = 1$) and computes the inverse of $e \equiv 1(mod\phi(n))$ and makes (n, e) public to recieve messages and keeps (p,q,d) private. RSA derives their security based on factoring integers and solving the discrete log problem being in a class of hard problems. Next we need to briefly describe Diffie-Hellman key exchange[19], this was established in 1976 and it lets Alice and Bob generate a key without sending it across an insecure channel and the process is this: one of them chooses a prime and a primitive root (A integer $g \in \mathbf{Z_n^*}$ is a primitive root modulo n if $ord_n(g) = \phi(n)$ where the order is the smallest integer k such that $a^k \equiv 1(modn)$ where the $gcd(a, n) = 1$) then makes the values of p and g public then. Alice sends across $g^a modp$ where $a \in 1, 2, ..., p-2$ and Bob sends across $g^b modp$ where $b \in 1, 2, ..., p-2$. Finally both of them compute $K = g^{ab} modp$ and they have their key. I believe we now have enough prerequisite information to start looking at a few algorithms and exploring the possible ethical issues.

5 Methods

5.1 Shor's Algorithm

Shor's Algorithm is a polynomial-time (big oh of some power of the input) algorithms for prime factorization and discrete logarithms. On a normal computer prime factorization and the discrete log problem are considered in the class of hard problems. The expensive part (with respect to space and time complexity) of the algorithm is the modular exponentiation. Modular exponentiation is given n, r and g find $g^r(modn)$, these have 2 classical algorithms to solve this is either repeated squaring or fast modular exponentiaion (compute all the exponents from $1tor$ and reduce modulo n as you go). As Shor states[16] the best one to use is repeated squaring since its linear $O(N)$ multiplications and squarings for a N-bit number mod n. We can use Schönhage–Strassen algorithm for integer multiplication of large numbers for this quantum gate which runs in $O(l^2 log(l) log(log(l))$ and for relatively small numbers we would just use regular old boring multiplication. The technique for computing $g^a \ mod(n)$ is first, apply repeated squaring to get a number of the form $g^(2^i)$ then we multiply together the powers obtained previously. Returning to how we defined the modular exponentiation, we only need to compute $g^r(modn)$ where g is fixed and r is in

superposition, this means that we can use a gate array and have r as input and fix g and n. This has pseudocode

---

a := 1
for $i = 0 -> N - 1$
if (i == 1) then
$a := ax^(2^i)(modn)$
endif
endfor

Now that we have a methodology to perform modular exponentiation, we can look at prime factorization, in which we consider how to factor any number in the integers into a product of primes. Shor's algorithm runs in $O((log(N)^2)log(log(N)(log(log(log(N)))))$. We do not actually factor N directly, we find the least integer r such that $x^r/equiv1(modn)$ this value is commonly called the order of an element. The steps of factoring N are, choose a random integer $x(modN)$, find its order r and compute the $gcd(x^(r/2) - 1, n)$, since $(x^(r/2) - 1)(x^(r/2) + 1) = x^r - 1 \equiv 0(modN)$ however, the $gcd(x^(r/2) - 1, n)$ fails to be a factor of N if the order is an odd number $(2k + 1, k \in \mathbf{Z})$. Therefore, this gives us a method to factor N, now we need to go about constructing a method to use a quantum computer to perform this procedure. To do this we use two registers which hold the integers (x and N). First we want to calculate a q such that its a power of 2 between $N^2 \leq q \leq 2N^2$. In our quantum gate array we do not need to store N, x or q in memory as they will be build in instead. We then put the first register into superposition representing the numbers $a(modq)$ and put each bit in the first register into superposition. We then calculate in the second register $x^a(modN)$ then perform the Fourier Transform on the first register (this creates our unitary matrix) and following some summations and integration that the paper goes into great detail about we will get the value r that we desire, so basically factoring N boils down to finding the order. Next we need to consider to how calculate discrete logarithms. The discrete logarithm of an integer x with respect to p and g is the integer r with $0 \leq r < p - 1$ such that $g^r \equiv x(modp)$ and all we need to do on a quantum computer to solve this is 2 modular exponentiation and 2 Fourier transforms and have 3 registers this follows a similar idea to what we have already discussed in this section so the implementation will not be discussed. Shor does discuss in the paper that this algorithm to factor integers and calculate discrete logarithms does thwart public key cryptosystems (e.g. RSA). It is easy to see how RSA is affected by this, we can calculate a factor reasonably quickly as seen above which means that given $N = pq$ where p and q are integers that once we find one of them by simple division we can find the other since N was a part of the public key then $phi(N)$ can be easily calculated which means all Eve (the eavesdropper) has to do is then do the same steps that either Alice or Bob did to create their public key to get all the information to not only create messages as that person but decrypt messages as Eve would have access to all of the information. This poses a serious privacy concern since not only

could Eve decrypt private messages not intended for them but they could pose as one of them and send messages acting as that person. We are next going to consider a newer algorithm this one is for solving systems of linear equations.

5.1.1 Schönhage-Strassen Algorithm

This algorithm was invented in 1971 by Volker Strassen and Arnold Schönhage, its a divide and conquer strategy using the convolution theorem in mathematics. This theorem, divides a number into n elements where each element consists of an equal number of bits (padding with extra zero's at the end may be needed)we then regard them as vectors and apply convolution to them which basically multiplies them together in a fancy way, this works efficiently for large numbers.

5.2 Quantum Algorithms for Systems of Linear Equations

This algorithm is more recent then Shor's Algorithm, this came from 2015 from Aram W. Harrow. This algorithm solves the problem of finding solutions of the equation $Ax = B$ where A is a rectangular matrix and $x \in \mathbf{C}^N$ where $\mathbf{C}^N$ is vectors whose entries are complex numbers $a + bi$, "the output of this algorithm is a quantum state on $log(N)$ qubits whose amplitudes are proportional to the entries of x."[7] The key is that b is given as a quantum state, it also should be stated that the matrix A can be row reducable. The key result is that when you put the input and output in a quantum state this achieves "finding x in time sublinear, or even polylogarithmic".[7] The key difference in this is that classical algorithms for solving linear systems will "output the entire vector x as a list of numbers while the quantum algorithms output the state whose N amplitudes are equal to x. A thing to remember is that this algorithm will be the some piece in a larger algorithm, so to list some applications of this one is to list some applications of systems of linear equations the most interesting one is machine learning. In machine learning a "widely used application of linear systems is to perform least squares estimation"[7] to predict values of parameters. Harrow did not mention any possible ethical issues that could arise from this algorithm and it is understandable because he does mention that "linear system solving is usually a subroutine in a larger algorithm" and it "applys to a variety of settings".[7] I agree with him it varies from situation to situation this does not go out to solve any one major problem this solves a smaller problem which usually is just a small chunk of a larger problem. However, once it is in relation to a problem like machine learning then I think that it shares the same ethical issues that the bigger problem has. We are next going to consider another early algorithm Grover's Algorithm.

5.3 Grover's Algorithm

Grover's Algorithm or as its paper is called is "a fast quantum mechanical algorithm for database search",[6] this algorithm is significantly faster than any classical algorithm can be. This algorithm has requirements that the database

containing N items is unsorted and only one item in the database statisfies some requirement and that one item is then retrieved. Classically the only way to do this problem with the unsorted database is to iterate through the contents of the database scanning each individual item as you iterate. We know on average this requires $\frac{N}{2}$ iterations on average and N in the worst case. Let a system have $N = 2^n$ states, these 2^n states are represented as n bit strings, we want to find a unique state S_v that satisfies the condition$C(S_v) = 1$, and all other states S, $C(S) = 0$ So "the problem is to identify the state S_v".[6] The algorithm has the following steps, you first initinalize the system so that all N states have the same amplitude. The next step is that we "repeat the following unitary operations $O(sqrt(N))$ times"[6] we let the system be in any arbitary state, we will denote the state by S: if $C(S) = 1$ then we apply a rotation to the phase state, if $C(S) = 0$ we do nothing to it; then we apply some "diffusion transformation D"[6]. Then we sample the resulting state if $C(S_v) = 1$ then we have our final state. Now something interesting was done, we applyed a rotation transformation in the first part of this loop, to achieve this pratically we would have "one portion of the quantum system sensing the state and then deciding whether or not to rotate the phase"[6]. This does not involve a measurement. An interesting thing to note is that this "search algorithm does not require any knowledge about the problem"[6], it can easily be applied to different databases without any modification required. This algorithm is also very simple compared to other quantum mechanical algorithms. One thing to note is that like Harrow above Grover does not mention any ethical issues that might be associated with this algorithm and unlike the Harrow's algorithm for solving systems of linear equations this one does have direct conflicts because this algorithm is very efficient in searching through unsorted data $O(sqrt(N))$ meaning that for example if you had a database full of personal financial information all it would take on average is square root time which is fast. Which has major privacy concerns especially if the data that is kept in that database is not secure or encrypted in someway that cannot be broken by Shor's Algorithm which we know already can easily break RSA, so in theory you could combine this Shor's Algorithm to break the encryption of the database if its encryption in anyway involves factoring large integers or solving discrete logs being in the class of hard problems and then apply Grover's algorithm to find whatever you need to find from the un-encrypted database. We are going to move on to our next algorithm which is a verification algorithm and a interesting application of it a quantum locker.

5.4 Verification Algorithm and Quantum Locker

This section is going to not only be a discussion on an algorithm this will also be a discussion on the whole process of a quantum locker just so we have some context for this whole situation because before we have had an idea about the application of the algorithms we have looked at so far. This algorithm is a little bit different this one is a verification algorithm to "process the scheme of a Quantum Locker, a protocol in which any legitimate party can verify his/her

authenticity by using a newly developed Quantum One-Time Password and retrieve the necessary message from the locker"[3] this is actually supposed to increase security. "This algorithm uses a verification box V"[3] in order to distinguish between two states which geometrically are not orthogonal to each other. Next, we need to discuss what exactly the process behind a quantum locker is and what is expected of a one-time password. The quantum locker has three stages. One, a message and conditions for verification with the OTP (One time password) are inputted to the locker. Two, the state of the OTP is quantum teleported to the intended receiver. Finally, a protocol is presented where verification of the OTP is required so that the message can be read. However, the OTP has to have the following properties: "verifiability" (the message can be verified by the receiver) and "unforgeability" (the message can not be forged). The process behind the locker is it consists of m qubits which store the message and "one ancillary qubit, which are inaccessible to any outside party"[3] it also has an "input slot for the password. Now we have to discuss if there is any ethical issues surrounding this application and algorithm, because of the quantum locker and the one time pad this actually increases security because the password and it achieves a key aspect in cryptography verifiability and unforgeability meaning that a third party can not tamper with the message in any way shape or form. So therefore, I do not see any ethical issues in this, in fact this is a very strong level of security. The authors also go through and prove the security aspects of this process, which is a really positive thing because currently the only other paper which considered the implications of their work is Shor. However, an ethical issue still exists and through this increased security and measures to protect messages, as this becomes closer to reality, who is going to apply this and are their intentions good or bad we don't know at this point if someone transfers credit card information across password protected with only the person on the other side being able to not only recieve the message but also input the password. We are next going to consider the earliest algorithm the Deutsch-Jozsa Algorithm.

5.5 Deutsch-Jozsa Algorithm

The Deutsch-Joza Algorithm is this: say we are given a function $f : 0, 1^n -> 0, 1$ where $n \in \mathbf{Z}$ then Deutsch-Joza algorithm says that one of two possibilities holds: either f is constant, which implies that either $f(x) = 0$ for all $x \in 0, 1^n$ or $f(x) = 1$ for all $x \in 0, 1^n$ or it is balanced which implies that the number of inputs $x \in 0, 1^n$ for which the function takes the values 0 and 1 are the same. In the classical case with a small number of inputs. This is actually an easy problem, its just calculating the value of a function at an point between 2 endpoints so in the worst case you may need $2^{n-1} + 1$ queries. In the quantum case we only need one calculation. The algorithm is this, we have n bits resulting from measurements and if they all equal 0 then the function is constant; however if at least one measurement is 1, we conclude the function was balanced, so therefore all you need is two qubits, apply a mathematical transformation to their multiplication and you are done. So it is the easiest

algorithm we have considered computationally. It does not immediately jump out what the application of this is however, think back to earlier on when we discussed Grover's algorithm we were checking in that case if there was a unique state S_v that satisfies the condition$C(S_v) = 1$, and all other states S, $C(S) = 0$ and it turns out that so this algorithm would be applied in that search[20]. Therefore, the ethical issues surrounding this algorithm once again only have to do with the applications of it because unlike Shor's and Grover's this does not have a goal to solve some problem from the outset. Next, we are briefly going to discuss another algorithm for discrete logs and RSA integers however, we are not really going to talk about the idea or the process behind this algorithm we are going to really just see if this algorithm from February 2, 2017 goes into more detail about the ethical issues then Shor did 20 years earlier.

5.6 Algorithm for Discrete Logs and RSA integers

This part will be handled very differently than any other algorithm we have considered up to this point, rather than going through any of the rationale we will rather consider right away if the authors considered any of the ethical issues surrounding an algorithm to not only calculate discrete logs but also factor RSA integers and the authors do mention in section 5.1 of the paper that "Quantum algorithms for computing short discrete logarithms may be used to attack certain instantiations of asymmetric cryptographic schemes" [5] and rather than just say that this factors large integers they just outright say that this factors RSA integers which is the exact same as Shor in that regard since way back in the 1990's he already mentioned this. Next, we are going to consider quantum information set decoding algorithms. .

5.7 Quantum Information Set Decoding Algorithms

This algorithm looks at the security of other cryptosystems who relies not on factoring large integers but however decoding a linear code, an example of this idea is what is called "Syndrome Decoding Problem"[11] which is given H and $s^T = He^T$ where $|e| = w$ find e where H is a full rank binary matrix of siz $(n-k)xn$ this algorithm actually combines together Grovers search algorithm with a few others by Bernstein, Jeffery, Lange and Meurer which we are not going to cover to solve this problem. Howver, this is as deep as we are going to go with this algorithm because of how mathematically intense this is and that is beyond the scope of this paper. So we have to now ask through this process do the authors mention any ethical issues surrounding this algorithm and sadly they don't and there is a major one because this is targeting a different variety of cryptographic system. Then there is a major privacy concern associated with it. Next, we are going to consider our last algorithm which is not as mathematically intense as this one, a quantum algorithm for the closest vector problem.

5.8 A Quantum Algorithm for the Closest Vector Problem

This algorithm has applications in computational linguistics and is critical to "many tasks such as clustering, text classification, phrase/word similarity and sentiment analysis" and this "determines the closest vector to $\vec{s}$ out of some set of N-dimensional vectors."[22] So in other words "given vector $\vec{s}$ and a set of M vectors $U = \vec{v_0}, \vec{v_1}, ..., \vec{v_{M-1}}$ the closest vector problem is which $\vec{v_j}$ has the smallest distance with $\vec{s}$" [22]. In the classical case direct calculation of the smallest vector would have complexity $O(MN)$, (where M, N correspond to what we have defined them as before) so it is desirable to find a quantum algorithm; however, there is 2 major assumptions for this to work: both vectors $\vec{s}$ and $\vec{v_j}$ are d-sparse (no more than d non-zero entries) and both of them are also normalized. This algorithm gives a significant improvement even if M is very large to get $O(\sqrt{NM}log(M)d^2r_{max}^4)$ where r_max is greater than or equal to the maximum distance of an arbitrary vector in the set, and d is how sparse it is. So now that we have seen the difference in the time complexity we now have to ask the question what are the ethical issues, and like we have seen before the issues have to do with the application of the algorithm not the actual algorithm, and this algorithms applications lie in computational linguistics and like before we have to ask, where is this being used if it is being used in sentiment analysis then it has some major issues since then something that you write, the feeling and the choice of words can behind it can be used against you. We are finally finished with the methods section and are going to go on to talk about a related work that was found during the research process of this report.

6 Related Works

Through the research process I stumbled across a paper by Ronald de Wolf titled "The Potential Impact of Quantum Computers on Society" which covers the same issues that have been presented already. Like Shor breaking RSA and Diffie-Hellman and Grover's search algorithm. This is a good thing since there are other people out there considering the ethical issues that these algorithms have. We are now going to move on to the discussion section where we will bring together all the ethical issues that we have been discussing so far and then draw some conclusions based on our observations thus far.

7 Discussion

So to reiterate Shor's Algorithm poses a serious privacy concern since not only could an eavesdropper decrypt private messages (if they are encrypted in RSA or have key made by Diffie-Hellmen) not intended for them but they could pose as one of them and send messages acting as that person since it can factor large integers and calculate discrete logarithms. However, Shor did bring it up in his paper that this algorithm to factor integers and calculate discrete logarithms does thwart public key cryptosystems and 20 years later in the algorithm for

Discrete Logs and RSA integers section the authors do still mention the same points that Shor does bring up about privacy concerns and a key thing they do right away is mention in the title that this factors RSA integers which is very good since even after 20 years authors keep mentioning the same security concerns that quantum computers are going to have because of how quickly they can break asymmetric cryptosystems when you apply these two algorithms. There is also Grover's search algorithm which allows you to search through an unsorted database which shares alot of similarities with this group of algorithms the ethical issues are really apparent because what type of database are you searching through and what exactly are you searching for. Then we discussed algorithms whose intentions were to find some vector or determine the nature of a function (Deutsch-Joza) and we concluded in these cases that these algorithms have no apparent ethical issues, however, ethical issues arise when you consider the applications of these algorithms. The key difference between the ones we listed earlier and these ones are the ones like Shor's make their ethical issues known and they are easier to determine (e.g. factoring large integers are the back bone of RSA) and the other ones have more pure mathematical intentions determine the nature of a function, the shortest distance of a vector. These ones are harder to determine since its applications have the issues. Then we looked at a verification algorithm and the quantum locker which intends to increase security through the One Time Pad which is nice but who is going to apply this and are their intentions good or bad we don't know at this point if someone transfers credit card information across password protected with only the person on the other side being able to not only recieve the message but also input the password. There is a common theme between all these algorithms we have looked at and that is like a classical computer the ethical issues lie in the applications of these algorithms not the algorithms themselves, for example, if you just look at Shor's algorithm from a mathematical point of view its not unethical, it finally gives an efficient polynomial time algorithm to factor integers and compute discrete logs.

8 Conclusion

The common theme that we have seen is quantum computing like classical computing has no special unique ethical issues, its issues lie in how you apply the computer. I mentioned back in the motivation section that I really wanted to see the intersection between quantum mechanics, mathematics and computer science and it was really interesting to see the speed up of computing discrete logs. The implications of Shor's Algorithm and Grover's Algorithm are not as exciting as they originally were to me because of how much our security relies on factoring, and so on however reading how these algorithms work technically is really cool since its all transformations and rotations. Quantum computing is going to be a exciting field as of writing this IBM already has a 50 qubit quantum computer and thankfully up to this point ethical issues have been considered not only by the authors of the papers but also people like Ronald de

Wolf are bringing together papers and generalizing these issues.

References

[1] Scott Aaronson. The limits of quantum computers. *Scientific American*, 298(3):50–57, 2008.

[2] Dorit Aharonov. Quantum computation . pages 1–78, 2008.

[3] Bikash K. Behera Avinash Dash, Sumit Rout and Prasanta K. Panigrahi. A verification algorithm and its application to quantum locker in ibm quantum computer. page 9.

[4] Ronald de Wolf. The potential impact of quantum computers on society. *Ethics and Information Technology*, 0(0):1–6, 2017.

[5] Martin Eker and H Johan. Quantum algorithms for computing short discrete logarithms and factoring RSA integers. pages 1–15, 2017.

[6] Lov K. Grover. A fast quantum mechanical algorithm for database search. *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC '96*, pages 212–219, 1996.

[7] Aram W Harrow. Quantum Algorithms for Systems of Linear Equations. pages 2–4, 2015.

[8] IBM. Now testing: prototype 50 qubit processor.

[9] IBM. What is Quantum Computing.

[10] Israel Koren. A. The RSA Encryption Algorithm.

[11] Ghazal Kachigar and Jean-pierre Tillich. Quantum Information Set Decoding Algorithms. pages 1–20.

[12] Rosen Kenneth. *Elementary Number Theory & its applications*. Pearson, 2011.

[13] Theo Kortekaas. TOP: Multiplying large numbers and the Schönhage-Strassen Algorithm. (february):1–51, 2015.

[14] Ashley Montanaro. The past, present, and future history of quantum computing. (November), 2015.

[15] University of Waterloo. What is Quantum Computing 101.

[16] Peter W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. pages 124–134, 1995.

[17] Umesh Vazirani. Quantum Computation. 2004.

[18] Wen Wang, Xu Jiang, Liang-zhu Mu, and Heng Fan. A quantum algorithm for greatest common divisor problem. pages 3–7, 2017.

[19] Wade Trappe Washington and Lawrence C. *Introduction to Cryptography with Coding Theory 2nd Edition*. Pearson-Prentice Hall, 2006.

[20] John Watrous. Lecture 5 : A simple searching algorithm ; the Deutsch-Jozsa algorithm. *Quantum*, pages 1–6, 2006.

[21] Wikipieda. Sentiment Analysis.

[22] William J Zeng. The Abstract Structure of Quantum Algorithms.