Designing a Practical Quantum Network Using Standard Basis Rotation and Blockchain Verification[1]

Evan Meade – evanm831@gmail.com

Keystone School, San Antonio, TX

Three years ago, I was sitting on the couch reading a copy of *Wired* magazine when I stumbled upon an article that simply blew my mind. The device it described and the concepts it explored seemed so outlandish that, at first, I actually thought it must have been describing the premise of a sci-fi movie. It talked at length about devices whose interiors were orders of magnitude colder than interstellar space. Then it discussed how a handful of particles at the heart of the machine could exist in multiple realities simultaneously, binding and unbinding from each other in complicated ways. It claimed that even *measuring* this fragile arrangement would be enough to destroy it. And finally, it said that somehow all these bizarre aspects added up to make a “quantum” computer! I have no shame in admitting to having never felt so confused in my life. How can you have data that’s two things at once? What good is an answer that breaks when you read it? Why would you even bother building such a strange and complicated machine? I quickly became obsessed with these questions and this subject in general.

In the weeks that followed, I scoured the web finding other articles on the subject, and I read every one I could find. It was through this experience that I discovered there’s a difference between knowing and understanding when it comes to science. I could rattle off some definitions and statistics easily, but they were still just words to me. It wasn’t until I bought some books on

[1] This is an abridged report. For full technical details, contact the author at the listed email address.

quantum information that I started to truly absorb some of that knowledge. The first book I read was *Quantum Algorithms via Linear Algebra* by Kenneth W. Regan and Richard Lipton, and it was HARD. You see, almost everything in quantum mechanics is described through vectors and matrices, and I had never even seen those before. However, as challenging as it was to try and teach myself about these new mathematical forms, the subject was always interesting enough to me to make it worthwhile. As I progressed and read other books, the math started to become more comfortable for me. I began to understand how a vector can represent a quantum state, and how a matrix can describe a transformation. I started to play around with some simple quantum states on paper, just to see what I could make them do. After about a year of honing my understanding of quantum information, I finally knew enough to come up with my own research question on the topic. I asked myself, what's the most efficient way to send information securely on a quantum state? Essentially, I wanted to devise a way to "encrypt" information using quantum mechanics, but in a more efficient way than other researchers had done. Because I was trying to research in such a young field, most of my work in the beginning was purely theoretical. I worked by myself at home with a notebook, scribbling ideas and then scribbling over them when they didn't work out. Sometimes I would email random physics professors and show them what I'd done so far to see if they could find holes in my idea. Again, during this time my results consisted entirely of mathematical theory. However, in these last few months I've actually been able to gain some experimental data by reaching out to companies and using their simulation software. I even got to run some programs on one of IBM's quantum computers! It's truly amazing how many people are willing to help you if you ask nicely.

Through all this trial and error, it has taken me two years to refine my ideas into a form I think is finally solid, and that final form is described below. Though there's still more I'd like to do with it, I'm happy with what I've done so far. I know it's a cliché, but the journey really has been more fun than the destination. The experience and knowledge I've gained by working with vectors, programming computer simulations, and even just understanding the background for my project is invaluable. However, the fun I've had pursuing this project has meant even more to me. I would encourage everyone to go outside of their comfort zone and explore things you don't understand, because you never know what you'll find in the process.

Abstract

Last year, the researcher outlined the mathematical basis of a new quantum secure direct communication (QSDC) protocol. QSDC protocols are methods of information transfer which gain security from the use of quantum mechanical effects. Due to the measurement principle, quantum communication reveals eavesdroppers with a probability arbitrarily near unity. In a world where traditional encryption is increasingly threatened by quantum computers and Shor's Algorithm, QSDC protocols provide impregnable security to banking transfers, diplomatic wires, and general communications. In contrast to existing QSDC protocols, the researcher's protocol does not require the use of entanglement, which can be technically difficult to create and maintain without succumbing to decoherence and collapse. Further, the researcher's protocol can be implemented with simple optical elements, transmits information directly, and retains quantum security advantages. Additionally, the protocol uses blockchain technology to aid previously unconnected nodes in conducting identity verification in order to initialize the quantum protocol. A rudimentary proof of concept was conducted last year with promising results. This year, the researcher developed the protocol by modifying a similar yet vulnerable protocol he created last year. In addition to mathematical verification, the researcher is taking advantage of new quantum information programming languages to mathematically simulate the

protocol and its results. Recently, IBM allowed the researcher to run trials on a real quantum computer, with a success rate above 90%. Given the promising results of the project, the protocol may soon be used to protect businesses, governments, and private citizens from certain types of monitoring, espionage, and cybercrime.

Background

Quantum Communication

A quantum system is any system which experiences quantum mechanics. A single quantum system's state can be described as a qubit; this is analogous to the information theory concept of a bit. A qubit's state can be described by a unit vector on the Bloch sphere:

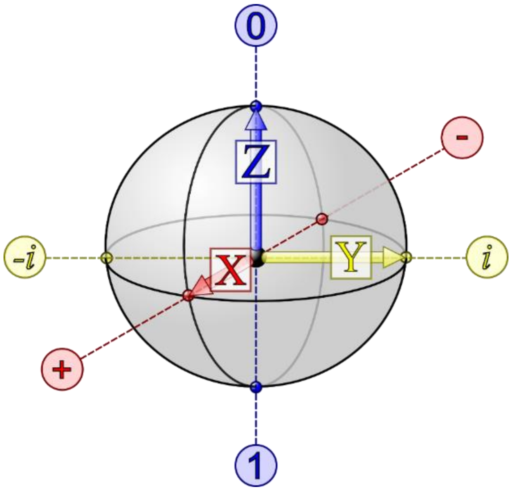

Figure 1 – Bloch Sphere

https://openclipart.org/download/142879/qubit-bloch-sphere.svg

Note that an arbitrary quantum state *Ψ* is denoted by the ket |*Ψ*>. Any measurement of the qubit must take place with respect to a diameter of the Bloch Sphere. If the state vector is coincident with the diameter, the result of the measurement is determinate as either 0 or 1. If the state vector of the qubit is not coincident with the measurement diameter, the measurement will probabilistically return a result of either 0 or 1.

A quantum information protocol (QIP) is an algorithmic procedure which takes advantage of quantum mechanics to exchange information between multiple parties in unique ways. The vast majority of QIPs are quantum key distribution protocols (QKDP), which create random encryption keys between multiple parties while detecting eavesdroppers. The first QKDP, BB84, was created by Charles Bennett and Gilles Brassand in 1984. In this QKDP, Alice wishes to share a random key with Bob while avoiding Eve from learning anything about the key as she eavesdrops (these are the customary names for a cryptographic protocol). Alice starts by generating two binary strings *a* and *b*. Alice sends a series of qubits (likely photons) to Bob using the mapping for $|\Psi_{ab}>$

$|\Psi_{00}> \mapsto |0>$ $|\Psi_{10}> \mapsto |+>$

$|\Psi_{01}> \mapsto |1>$ $|\Psi_{11}> \mapsto |->$

This mapping uses a_i to determine a diameter to encode b_i along. The red mappings represent the *z* or “standard” basis while the blue mappings represent the *x* or “Hadamard” basis. When Bob receives the qubit, he randomly measures each one either with respect to the standard basis or the Hadamard basis as determined by a random binary string *c*. The result of these measurements is a binary string *d*. Alice and Bob then compare *a* and *c* over a public classical channel. They discard all qubits in positions where *a* and *c* differ. They then compare a portion of *b* and *d*. If there are any discrepancies, they will know that Eve was eavesdropping. This is because there is no way that Eve can measure the qubits in transit without affecting their quantum state, and thus causing different measurements. Additionally, Eve cannot copy the qubits and measure the copies due to the No Cloning Principle. If they find no discrepancies during this comparison, they know with high probability that their communication was secure.

There are many other QKDPs which utilize different methods. However, by just looking at this one, some disadvantages may be evident. The most notable is that this protocol can only be used to create a *random key*; it cannot be used to transmit information directly. Another disadvantage to this system is that half of the quantum communication (on average) is discarded due to the 50% chance that Alice and Bob use the same basis. In this way, it is extremely inefficient. Finally, it depends on a classical channel in addition to a quantum channel. Yes, a quantum channel can be used to transmit classical information, but the fact that it is required in the first place is indicative of another inefficiency.

Distributed Ledger Technology and Blockchain

Distributed ledger technology and blockchain have been popularized in recent years due to their use in Bitcoin and other cryptocurrencies. By using cryptography, Bitcoin enables a form of decentralized, digital value transfer which is incredibly difficult to disrupt provided no attacker controls the majority of the network's computing power. However, the applications of blockchain technology extend far beyond value transfer. Blockchains can enable new forms of distributed computing, decentralized data storage, secure identity management, and other and other crucial processes.

Distributed ledgers are large lists consisting of data in the form of *blocks*, which are computationally infeasible to modify after they have been written. *Nodes* can append to the blockchain by broadcasting *transactions/entries* on a best effort basis. Nodes which are *mining* can group pending transactions into blocks. The blocks contain *hashes* which reference previous blocks. If they can solve a difficult computational puzzle, the nodes will broadcast the new block and it will be appended to the ledger. When this process is iterated, a chain of blocks called a *blockchain* is formed.

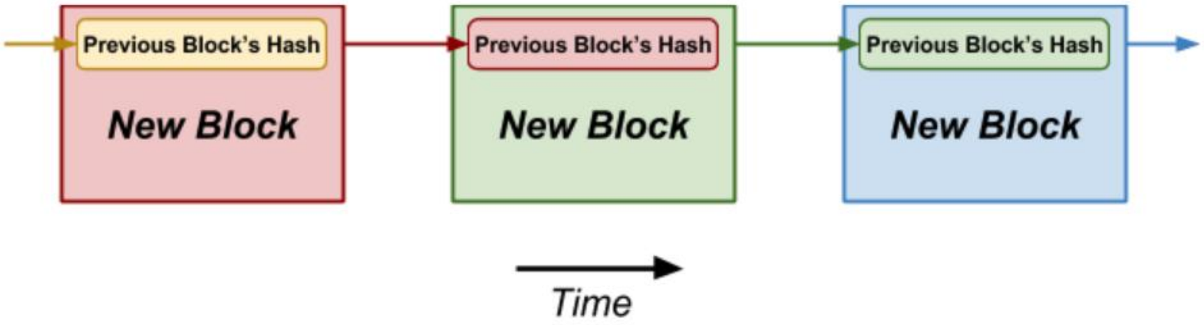

Figure 2 – Blockchain structure

In order for an attacker to modify data which has already been entered into the blockchain, they would have to redo the computational work of all subsequent blocks. Such an attack becomes exponentially difficult as new blocks are added. Because the *difficulty* of the puzzle is dynamically changed based on the total computational power of all miners, even a quantum computer is unlikely to dominate the mining process in the near future. Thus, blockchains may be considered a stable, secure form of data storage which could be employed by a variety of applications.

Results of Previous Year

The researcher was able to successfully create a fundamentally new type of quantum protocol which is more rapid, more secure, and more efficient than existing quantum protocols. The protocol is gained efficiency over existing protocols by encoding information directly on quantum states. By contrast, existing protocols often have Alice send a state to Bob, Bob tells

Alice which basis he used, Alice tells Bob which basis she used, and then Alice sends the encoded message to Bob. The researcher's protocol is also more secure than existing quantum protocols because in order for Eve to perform a man-in-the-middle attack, she must have knowledge of the last 225 bits sent from Alice to Bob. She cannot obtain these because she cannot even measure the encoded states since she never knows which basis they are working in. Finally, the protocol is clearly more efficient than existing quantum protocols because it utilizes every transmitted state instead of discarding half or more transmitted states on average. By satisfying these three criteria, the researcher has created a fundamentally new type of quantum protocol which is more rapid, more secure, and more efficient than existing quantum protocols. However, the protocol relied on classical cryptography to distribute the initial key. Therefore, in this year's project, the researcher designed a new protocol which used the same principles as last year's protocol, but which does not rely on classical cryptography in any way.

Purpose

The researcher's goal was to redesign his quantum communication protocol from last year to eliminate the need for classical encryption. Though last year's protocol, M16, succeeded in creating a rapid, secure, efficient method of information transfer by encoding information directly onto the quantum state. However, it required classical encryption to distribute the initial random seed. Therefore, the researcher aimed to reuse the principle of fractional rotation around the standard basis of the Bloch sphere while altering the protocol to remove the need for classical encryption in the initial key distribution.

Hypothesis

Based on the researcher’s success using similar methods last year, the researcher predicted that he would be able to create a better protocol this year that does not require classical encryption in any way.

M17: Final Protocol Design

By convention, quantum protocols are named based on the last name(s) of the designer(s) and the year of creation, thus giving the name M17. This protocol is designed to retain the security advantages of traditional quantum protocols while sending information in a much more direct and efficient manner. The general structure of a single exchange is shown below. The sending party, Alice, controls the transformations in the top line, while the receiving party, Bob, controls the transformations in the bottom line.

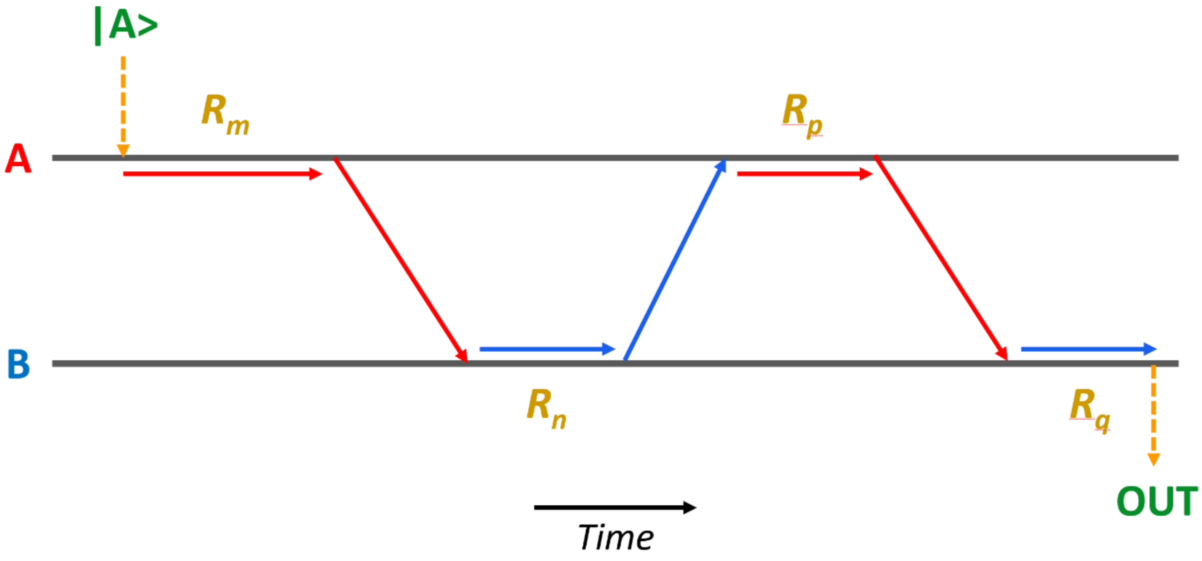

Figure 3 – M17 protocol diagram

There are two stages to the protocol, both of which follow this structure. First comes initialization, where the two parties establish a random seed, prove their identities, and expose any eavesdroppers. After that comes the encoding stage, where they can communicate normally using the seed they established in the first stage. Here's how a single bit is sent in the initialization stage, which closely mirrors the encoding stage:

1. **Alice** prepares a simple quantum state using the polarization of a photon. This state, |A>, is known as the antidiagonal polarization.
2. **Alice** rotates the quantum state by a secret amount in transformation R_m. This can be done using an optical device called a Pockels Cell.
3. **Alice** sends the photon to **Bob** using a special fiber optic cable such as a spun polarization maintaining fiber.
4. **Bob** rotates the state by a secret amount with R_n, implemented in the same way as R_m, and sends the state back to **Alice**.
5. **Alice** performs R_p, which undoes her random rotation from R_m and encodes a random bit onto the quantum state. **Alice** records this bit and sends the state to **Bob**.
6. **Bob** reverses R_n with R_q and measures the resulting state with a polarization filter and photomultiplier. Based on his measurement, he can determine which bit **Alice** encoded with her R_p transformation. **Bob** records this bit.
7. The above process is repeated 171 times.
8. **Alice** randomly selects 25 bits from the initialization process and posts them onto a special blockchain called Seedchain, which is used to prove identities and expose eavesdroppers.

9. **Bob** posts his measurements for the corresponding bits and posts 25 bits of his own, again drawing from the initialization process.
10. **Alice** posts her corresponding values for these bits.
11. If **Alice**'s measurements match **Bob**'s measurements with a certain percentage, they conclude that they are communicating with the correct person and no one has eavesdropped on their initialization process. They can now begin communicating normally.

Once initialization successfully occurs, Alice and Bob can communicate with actual information indefinitely. The process is identical to the initialization process except that R_p and R_q are modified to incorporate a pseudorandom bit which prevents certain types of man in the middle attacks. This pseudorandom bit is procedurally generated from the initialization seed and any transmitted messages.

Results

The researcher verified the protocol with three distinct methods: mathematical proof, computer simulation, and physical experimentation. In order to prove his protocol mathematically, the researcher simply described the quantum states and transformations using linear algebra and multiplied the correct combinations in order to find the theoretical result of measurement. Each case was demonstrated to lead to the intended measurement which represented the bit sent.

Next, the researcher used three quantum simulation packages: Microsoft's Quantum Development Kit, Rigetti Computing's PyQuil/Forest API, and IBM's Quantum Experience. The researcher translated the protocol into formats appropriate for each case. The Microsoft simulation ran 100,000 trials of sending a 1,000 bit message, and each case evaluated as expected; thus the correct information was conveyed by the protocol. Of course, this was an idealized simulation, so there was no noise or natural error, but these results nonetheless demonstrate that the protocol gives the correct result in every communication case it encounters. Next, each of the 64 cases encountered by the protocol were run with Rigetti's model in a single idealized trial, which again returned a perfect success rate of 100%. Finally, 8,192 trials were run on each of these 64 cases using IBM's simulation model, which also returned an overall success rate of 100%.

Recently, the researcher was able to obtain even more data validating his protocol in the form of experimental trials run on one of IBM's actual quantum computers, through the IBM Quantum Experience program. At least 1,024 trials were run for each of the 64 cases. The minimum success rate for a trial was 80.18%, the maximum was 98.83%, and the mean was 90.06%. The standard deviation of the success rate between trials was 5.45%. Based on current error rates in quantum computers, these are incredibly encouraging results which further attest to the validity of the researcher's protocol.

Conclusions

The researcher was able to successfully create a new quantum communication protocol which transmits information directly on the quantum state without necessarily requiring classical encryption in any way. The protocol is more secure than most existing encryption because it is resistant to attacks by quantum computers. It is also more efficient than quantum key distribution methods because it transmits information directly on the quantum state instead of merely establishing a random encryption key. As a further advantage over quantum key distribution methods, M17 uses all transmitted states instead of discarding half or more on average. Thus, M17 would provide the security necessary in a post-quantum world while also providing the efficiency and speed demanded by modern communications. Because the necessary components are well-developed, relatively inexpensive, and readily available, the protocol would be feasibly implementable in real world communications to protect businesses, governments, and private citizens from certain types of monitoring, espionage, and cybercrime.

In addition to the security and efficiency provided by the quantum protocol itself, the researcher was able to extend the protocol into a full scale network architecture by introducing blockchain identity verification. The security of distributed ledger technology rests on its being computationally infeasible to alter, even with a quantum computer. Although the Seedchain portion of the protocol uses classical signature schemes, they are provably secure with minimal assumptions and their difficulty is compounded by the continual addition of new blocks. Thus, not only would an attacker have to break this secure encryption scheme, they would have to do so within the average block time, which is a computationally infeasible task for the foreseeable future. Thus, by using appropriate parameters (signature scheme and proof-of-work), a blockchain can provide an easy way for previously unconnected parties to initiate a new quantum exchange of M17 by registering and verifying identities. When combined with the efficacy of the quantum protocol, M17 is able to provide an efficient, secure alternative to traditional encryption while requiring only basic optical instruments. Therefore, the researcher concluded that he met his original design goals as outlined in his Purpose.

Practical Applications

As the development of quantum computers rapidly advances, there is a growing need to adopt a new form of secure communication which is resistant to quantum attacks. However, such a communication method would also have to be efficient enough to support the high-bandwidth, low-latency demands of modern telecommunications. The researcher's design is able to do just that by gaining security advantages from quantum mechanical effects while transmitting information in a much more efficient and practical manner than existing quantum protocols. Thus, it is a prime candidate to supplant traditional encryption schemes in a post-quantum world. The protocol is particularly applicable to scenarios where security is of the upmost importance but speed is a close second priority. In particular, banking transactions, military communications, and diplomatic wires are incredibly sensitive transmissions which would benefit greatly from the methods outlined in this project. Additionally, due to the presence of blockchain identity verification, it is also reasonable to expect M17 to be used by individuals as other forms of privacy become obsolete. The Seedchain protocol allows for previously unconnected users to rapidly establish quantum communications with full authentication. This ease of secure connection between disparate parties is why M17 is a model of a network—such as the Internet—rather than merely a peer-to-peer communication scheme. Anyone with a quantum channel connection can begin interacting on a quantum-secure internet. Thus, by accounting for a range of connections, the researcher has developed a new of quantum communication scheme which will aid in addressing rapidly approaching security crises.

Future Expansion

The researcher has three major expansions planned for the project. First, he intends to expand upon the simulation methods which he has already used. These continuations include further trials and implementations on actual quantum computers. The former type of expansion applies to Microsoft's Quantum Development Kit, which was recently updated to include a more efficient simulation model which claims to be 4-5 times more efficient than the original model. This development would allow for a higher number of trials to take place which would further validate results already obtained. After these results are obtained, he will petition Rigetti Computing to grant him access to their quantum computers to gain even more experimental data regarding his protocol's efficacy. Comparison against the data from IBM's quantum computer may provide insight into how different quantum media affect the protocol's success.

Next, the researcher plans to further develop the Seedchain protocol in order to conduct a more precise analysis of its security. This development will introduce new details to its definition, such as setting block sizes, defining entry formats, and effectively scaling the computational difficulty. After these aspects have been set in place, the researcher will be able to program a simple test script which mines the blockchain and submits entries. By running this program on multiple computers on the same network, he will be able to analyze the blockchain's performance and stability. Any errors which arise will allow the researcher to correct them to further solidify Seedchain's security.

Finally, the researcher plans to implement a physical verification of the protocol. He has been in conversation with a researcher who may be able to provide lab space and equipment for a rudimentary test. When taken in conjunction with the mathematical proofs and computer simulations already established, the protocol would be able to be further verified and practical error rates established.

Works Consulted

Aaronson, S. (2013). *Quantum computing since Democritus*. Cambridge: Cambridge University Press.

Aggarwal, D., Brennen, G. K., Lee, T., Santha, M., & Tomamichel, M. (2017). Quantum attacks on Bitcoin, and how to protect against them.

Alexandroff, P. S. (2012). *An introduction to the theory of groups*. Mineola, NY: Dover Publications.

Amiri, R., & Andersson, E. (2015). Unconditionally secure quantum signatures.

Back, A. (2002). Hashcash – A denial of service counter-measure.

Buchmann, J., Dahmen, E., & Hulsing, A. (2011) XMSS – A practical forward secure signature scheme based on minimal security assumptions.

Cox, B., & Forshaw, J. R. (2013). *The quantum universe: (and why anything that can happen, does)*. Boston: Da Capo Press.

Dunphy, P., & Petitcolas, F. (2018). A first look at identity management schemes on the blockchain.

Feynman, R. P., & Zee, A. (2014). *QED: the strange theory of light and matter*. Princeton: Princeton University Press.

IBM (2016). IBM Q Experience.

Kiktenko, E. O. et al. (2017). Quantum-secured blockchain.

Larimer, D. (2014). Momentum – A memory-hard proof-of-work via finding birthday collisions.

Lipton, R. J., & Regan, K. W. (2014). *Quantum algorithms via linear algebra: A primer*. Cambridge, MA: MIT Press.

Microsoft. (2017, October 9). Setting up the Q# development environment. Retrieved January 15, 2018, from https://docs.microsoft.com/en-us/quantum/?view=qsharp-preview

Nakamoto, S. (2009). Bitcoin: A peer-to-peer electronic cash system.

Rieffel, E., & Polak, W. (2014). *Quantum computing: A gentle introduction*. Cambridge, MA: MIT Press.

Schneider, H., & Barker, G. P. (1989). *Matrices and linear algebra*. New York: Dover.

Shannon, C. E., & Weaver, W. (1964). *The mathematical theory of communication*. Urbana: University of Illinois Press.

Singh, S. (2000). *The code book: The science of secrecy from ancient Egypt to quantum cryptography*. Anchor Books.

Smith, R. S., Curtis, M. J., & Zeng, W. J. (2017) A practical quantum instruction set architecture.

Susskind, L., & Friedman, A. (2014). *Quantum mechanics: The theoretical minimum*.

Zhang, W. et al. (2016). Quantum secure direct communication with quantum memory.