Cryptography in Quantum Computing

Pam Choy and Dustin Cates
Florent Chehwan and Cindy Rodriguez, Avery Leider and Charles C. Tappert
Seidenberg School of Computer Science and Information Systems, Pace University
Pleasantville, NY 10570, USA
Email: {pc96111n, dc04381n,
fc87943n, cr84102n, aleider, ctappert}@pace.edu

***Abstract*—Quantum cryptography is an area of intense interest, as quantum computers contain the potential to break many classical encryption algorithms. With so much on the line, it is imperative to find a new quantum encryption method before quantum technology catches up with current cryptography. This study examines one of the very few experiments on encryption that has already been conducted and analyzes the results of the tests run on the IBM Cloud Server. It will attempt to recreate the sample experiment and make comprehensive adjustments for a real-world environment. This study will also look at the possible application of quantum public key encryption and the theoretical importance of quantum key distribution.**

***Index Terms*—quantum computers, quantum cryptography, quantum encryption, encryption algorithm, quantum public key encryption, quantum key distribution**

I. Introduction

The world of quantum computers is based on quantum theory, which largely deals with the behavior of particles at the atomic and subatomic levels. At these infinitesimal scales, the laws of physics, as scientists have grown accustomed, almost seem not to exist, or at least are drastically different.

In the case of quantum computers, the atomic particles are actual information. In a traditional computer, information is organized into series of transistors that, depending on the patterns of which they are on or off, form bits that can then be translated into binary. Each transistor can only represent a single state at a time: a 0 or a 1. In quantum computers however, a quantum bit (also known as a qubit) can be a 0, a 1, both, or somewhere in between. It is even capable of representing multiple states at the same time [18]. This state is known as superposition. The superposition of qubits is the fundamental factor that makes quantum computers vastly more powerful in comparison to a classical computer. However, the measurement of these states can oftentimes be difficult due to this superposition quality [13]. In quantum computers, the state of a qubit is stored in an atomic or subatomic particle using a variety of experimental methods.

Quantum mechanics, and therefore quantum computers, are anything but simple. Despite the complexity, the age of quantum computers is coming. With it will come a phenomenon popularly called the quantum break [5], which is a theoretical time when quantum computing will evolve to a point where it will render many common encryption algorithms obsolete [12]. Think about it. Many current encryption algorithms are based upon multiplying two very large prime numbers. This process, however, is reversible. These types of algorithms are not unbreakable but more accurately, not feasibly breakable because it would take current computers an unreasonable amount of time (sometimes decades or centuries) to break an algorithm or find a factorization. Because quantum computers are theoretically capable of computing at exponentially higher speeds, it is only a matter of time before today's strongest algorithms can be solved within minutes, therefore rendering these types of encryption obsolete.

While the quantum break has not yet occurred, theorists suggest that recent advances in quantum computing means that the quantum break is a highly likely scenario in coming years. With more and more of individuals' private data, e-commerce, and banking being done strictly through computers, the impending quantum break creates an urgent need for the knowledge and implementation of quantum encryption methods.

The goal of this research is to test a quantum algorithm cipher, using a simple example, on a real quantum computer, and then to identify what the obstacles are to understanding it. There are many jobs available, and unfilled, for quantum computing technologists who are capable of this task [1]. There are also very few courses of instruction offered, from PhD level to Master's level to Baccalaureate Level, because of the complexity of the subject.

The next section of this paper describes project requirements. A research study then continues with the next section on literature review related to this focus.

II. Literature Review

As more and more everyday transactions containing sensitive data migrate to a digital format, ensuring the safety of information has become more important than ever. As of now, complex algorithms are being used to secure information stored on computers and servers all over the world. Many, however, believe the age of quantum computing will bring this to an end.

As explained earlier, the emergence of the quantum computer will soon make most current methods of algorithmic encryption obsolete and insecure. One of the biggest problems security specialists are facing is the issue of key distribution [20]. Heavy investment is being made by major

Thanks to the IBM Faculty Award that made this research possible.

governments worldwide, such as the United States, European Union, and China. The United States Department of Defense has announced an $899 million research budget claiming the majority of that will be dedicated to quantum computing [15]. The European Union has announced a ten-year, billion-Euro plan to fund research that will turn quantum techniques into commercial products [2]. While official budgets are kept confidential, China has announced their plans for a billion dollar quantum research facility to be finished in 2020. They also claim to have launched the first satellite capable of quantum communications [16]. All three of these are showing clear goals to make significant advancements in the field of quantum mechanics and with these advancements, develop a new method to protect data from the enhanced abilities of quantum computers.

To date, while many theories exist, researchers have been unable to produce any concrete findings. Currently, it appears that the answer may lie in quantum public-key encryption (QPKE). In fact, significant strides have been made in a new method of encryption, known as quantum public-key cryptosystem. As detailed in ”A Practical Quantum Public-key Encryption Model”, a quantum public-key cryptosystem has the potential to be very efficient on a quantum machine, if implemented in conjunction with the ease of current asymmetric key distribution methods [17]. As ”The Race Towards Quantum Security” explains, quantum encryption through quantum key distribution (QKD) becomes a necessary step to ensure the security of information. In the purposed model, a QKD scheme would be implemented through the storage of information in quantum data carriers, known as qubits. This information would then be transmitted between two qubits via a quantum channel [9].

The term, ”Quantum channel” refers to the media for quantum information to be transferred during quantum entanglement. Quantum entanglement is when two qubits reflect the same state at the same time despite being separated by, theoretically, infinite distance. This would mean that even after the qubits are separated, if one qubit is changed, the second qubit will instantaneously reflect the same changes. Correlations between the two separated qubits cannot be explained without quantum mechanics. The simplest way to visualize quantum entanglement is through the use of Bell states.

$$\left|\Phi^{+}\right\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B\right)$$

Fig. 1a: Phi+ Bell State

$$|\phi-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A \otimes |0\rangle_B - |1\rangle_A \otimes |1\rangle_B\right)$$

Fig. 1b: Phi- Bell State

$$\left|\psi^{+}\right\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |0\rangle_B\right)$$

Fig. 1c: Psi+ Bell State

$$|\psi-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B\right)$$

Fig. 1d: Psi- Bell State

As shown above, Bell States can be represented by four different states: Phi+, Phi-, Psi+, and Psi- (Fig. 1). Out of these, the most studied state is Phi+. The expression Phi+, basically means that a qubit held by Alice (subscript ”A”) can be either 0 or 1. If Alice were to measure the qubit, the result would be random, meaning either possibility (0 or 1) would have the probability of 1/2. Similarly, if Bob (subscript ”B”) were also to measure his qubit at that moment, he would always get the same outcome as Alice. Therefore, when Alice and Bob communicated, they would find that, although their individual outcomes seemed random, they would be correlated with one another. This is partially why entanglement is believed by many to be the key to using quantum computing for encryption [3].

Theoretically, a Bell State expression could be used to securely create a key and send it from Alice to Bob using QKD protocol (fig. 2). Alice and Bob would start by sharing number pairs of entangled qubits. Alice would then send the qubits to Bob in different directions (vertical, horizontal, or diagonal left or right). Alice and Bob would then randomly pick and make local measurements of the qubits to ensure maximally entangled state (correlation). If they are not in correlation, then the photons will be discarded. In essence, the photons in the correct state would be translated into bits (for example, horizontal = 1 and vertical = 0) for Bob and thus produce a set of quantum keys for decryption. Even with the random outcomes, there is always correlation [3].

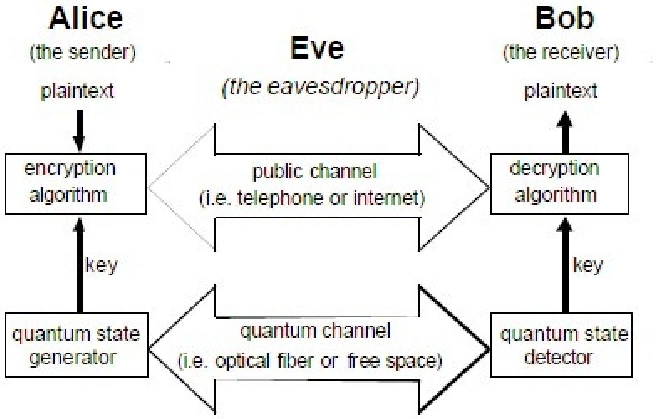


Fig. 2: Quantum Key Distribution

Additionally, quantum secure direct communication, also known as QSDC, is another proposed method of encrypting messages between Alice and Bob. QSDC is different from the QKD protocol mentioned above because, while both methods would generate a private key for the two parties to use in communication, QSDC does so without the need for key generation in advance [19]. With a QSDC scheme, a controlled-not (CNOT) gate is the primary method of encoding and decoding the messages passed between Bob and Alice. The key, in this case, is a ”sequence of two-photon pure entangled states ... [which are] reused with an eavesdropping check” so that an eavesdropper, such as Eve in figure 2, would be detected [19]. Each of these transmitted photons could theoretically carry one bit of the message being communicated.

It is also believed that quantum key encryption could be used to bolster the already quantum proof symmetric cipher schemes such as Advanced Encryption Standard (AES) [11]. However, a problem arises when considering key distribution for asymmetric cipher schemes which are currently expected to be broken by future quantum computers. To compensate for this problem, Wang and She propose that private keys be held by actual individuals and correspond to a single public-key that is created by a trusted third-party using the quantum computers already proven ability to generate truly random numbers [7], [17]. Through this process, the information would be secure and the plaintext would be unrecoverable from the cipher text. To break the cryptosystem, an individual would need to recover the private key from the public key, potentially giving them access to all messages of the intended recipient [17].

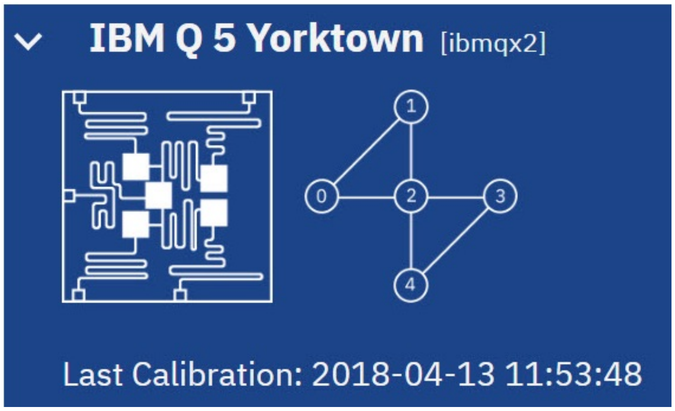
This intended attack however, would be theoretically impossible due to a law of quantum mechanics known as Heisenberg’s uncertainty principle. This law states that the position and velocity of an object, an electron for example, can not be measured precisely at the same time [4]. In the context of QKD and QSDC, this means that a third party would be unable to time the signal exactly in order to obtain the secured information needed to break the encryption.

Heisenberg’s uncertainty principle is not the only law of physics that is being relied upon to guarantee security. Lindsay believes that the ”no-cloning theorem of quantum informatics” will also play a role in securing or detecting potential attacks [11]. The no-cloning theorem is a widely accepted rule of quantum mechanics and essentially states that an arbitrary quantum state cannot be cloned [14]. This coincides with the even more widely accepted theory that one can change a quantum state simply by looking at it. As Lindsay applies it, this would mean that a quantum encrypted message could potentially be intercepted but the copying or reading of this message would actually change the state of the information, greatly increasing the likelihood that an eavesdropper would be detected.

While the quantum computer’s ability to generate random numbers would make the creation and distribution of cryptographic keys more secure, most current QKD models would suffer from a low rate of key generation on current machines, which would greatly limit the possibly of widespread distribution [10]. This limit is caused by the operation of current quantum computers which encode a single qubit to a single photon. As Lai *et al.* explain, there is currently a solution to this problem involving changes to the QKD protocol itself but it is far from cost effective. Despite multiple theories floating around the computer science and physics communities, a cost effective solution to QKD has yet to emerge.

III. Project Requirements

1) QC Set-up Instructions/QISKit
2) Registration and API key from IBM’s Quantum Experience
3) Operation Systems: Windows and Mac OS
4) Software Development Kit: QISkit and The Composer



IBM Q 5 Yorktown [ibmqx2]

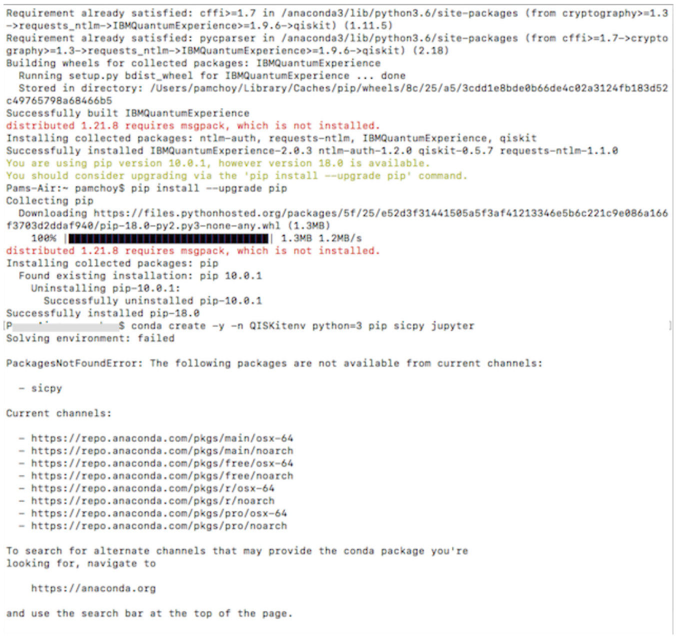
Last Calibration: 2018-04-13 11:53:48

Fig. 3: IBM Qx5

In order to conduct this project, it was necessary to have access to quantum computers. The experiment made use of the public access recently granted by IBM to a 5-qubit superconducting device (fig.3) via their ”Quantum Experience” cloud service. This service made use of two software development kits in the initial phase of the project: the IBM composer and QISkit. The Composer is IBM’s graphical user interface for programming a quantum processor while QISkit is an open-source framework for quantum computing with Python. The end experiment most heavily utilized the composer but QISkit was also important to the experience.

Once successfully installed, a user must register with IBM’s Quantum Experience website in order to start using the IBM Q Experience and QISkit to run programs on the remote back-end provided by IBM. A user can register by creating a log-in using an email address or other social media account such as Linkedin. The subscription is free for all users. After registering to the ”Quantum Experience,” IBM provides an API token that will be saved in a file called qconfig, which is passed to the program. This sets up a connection to the back-end server. It will then be possible to select a back-end server from those available on the IBM Q Experience, run the program, and get the results of the program.

A Quantum Computing source repository is available on Github to explore tutorials, run programs, and contribute to the



```
Requirement already satisfied: cffi>=1.7 in /anaconda3/lib/python3.6/site-packages (from cryptography>=1.3
->requests_ntlm->IBMQuantumExperience>=1.9.6->qiskit) (1.11.5)
Requirement already satisfied: pycparser in /anaconda3/lib/python3.6/site-packages (from cffi>=1.7->crypto
graphy>=1.3->requests_ntlm->IBMQuantumExperience>=1.9.6->qiskit) (2.18)
Building wheels for collected packages: IBMQuantumExperience
  Running setup.py bdist_wheel for IBMQuantumExperience ... done
  Stored in directory: /Users/pamchoy/Library/Caches/pip/wheels/8c/25/a5/3cdd1e8bde0b66de4c02a3124fb183d52
c49765798a68466b5
Successfully built IBMQuantumExperience
distributed 1.21.8 requires msgpack, which is not installed.
Installing collected packages: ntlm-auth, requests-ntlm, IBMQuantumExperience, qiskit
Successfully installed IBMQuantumExperience-2.0.3 ntlm-auth-1.2.0 qiskit-0.5.7 requests-ntlm-1.1.0
You are using pip version 10.0.1, however version 18.0 is available.
You should consider upgrading via the 'pip install --upgrade pip' command.
Pams-Air:~ pamchoy$ pip install --upgrade pip
Collecting pip
  Downloading https://files.pythonhosted.org/packages/5f/25/e52d3f31441505a5f3af41213346e5b6c221c9e086a166
f3703d2ddaf940/pip-18.0-py2.py3-none-any.whl (1.3MB)
    100% |████████████████████████████████| 1.3MB 1.2MB/s
distributed 1.21.8 requires msgpack, which is not installed.
Installing collected packages: pip
  Found existing installation: pip 10.0.1
    Uninstalling pip-10.0.1:
      Successfully uninstalled pip-10.0.1
Successfully installed pip-18.0
P[redacted]$ conda create -y -n QISKitenv python=3 pip sicpy jupyter
Solving environment: failed

PackagesNotFoundError: The following packages are not available from current channels:

  - sicpy

Current channels:

  - https://repo.anaconda.com/pkgs/main/osx-64
  - https://repo.anaconda.com/pkgs/main/noarch
  - https://repo.anaconda.com/pkgs/free/osx-64
  - https://repo.anaconda.com/pkgs/free/noarch
  - https://repo.anaconda.com/pkgs/r/osx-64
  - https://repo.anaconda.com/pkgs/r/noarch
  - https://repo.anaconda.com/pkgs/pro/osx-64
  - https://repo.anaconda.com/pkgs/pro/noarch

To search for alternate channels that may provide the conda package you're
looking for, navigate to

    https://anaconda.org

and use the search bar at the top of the page.
```

Fig. 4: Activate QISkit Error Message

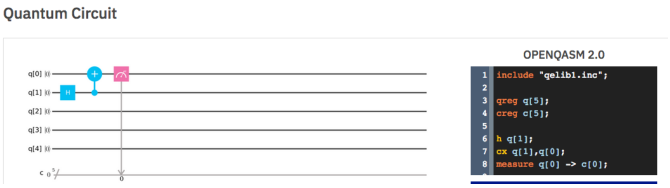
development of quantum computing by addressing important issues.

IV. Methodology

Resources to learn quantum computing and simple experiments are available in the IBM Quantum Experience, the Jupyter Notebooks, and the JupyterLab. These are primordial when learning to understand the structure of the program behind the more approachable graphical representation in the IBM Composer. The three steps of the development of a quantum program are the same as a classic program with the following functions: build, compile, and run. The first step, build, consists of creating a quantum circuit composed of quantum registers and adding gates to it in order to use and manipulate the registers. These gates will perform directly on qubits. The different back-end servers available can then be chosen during the compile step if, for example, it is desirable for the code to be executed on a quantum simulator, on the local machine, or on an IBM quantum chip. After running the code in the final step, and receiving a result, the user can select a variety of options that can affect execution of the code.

In preparation for the experiment, the Composer was tested to better understand how to program the score which can be run via the simulator or on the real hardware of QISKit. One thing that made the Composer easier to learn, was its graphical representation of QASM, a simple text-format describing quantum circuits (fig.5). The Composer provides tabs to drag and drop gates, barriers, and measurements onto the score or to apply them to the entire QASM code. It also gives options to either run the score against the actual hardware or in simulation mode.

The effect that the previously mentioned gates can have on qubits is sometimes described using a Bloch sphere. The diagram below (fig.6) depicts a simple Bloch Sphere where the 0 Vector (|0>) on the North Pole means low energy and 1 Vector (|1>) on the South Pole means active energy. The gates cause the qubits to go in different directions. In our experiment, the qubit was placed into superposition using a Hadamard gate, which transformed the qubit from the standard basis elements (North-South) to a new basis on the equator of the sphere (East-West) in which the probabilities of observing a 0 or a 1 would be simply 50 percent. Then, a Controlled-NOT gate was placed on q0 to generate entanglement. Lastly, a measurement was applied. Due to the fact that quantum computers process, but do not measure, classical bit state (0 or 1), a measurement must then be applied when running the simulator (fig.7).



```
include "qelib1.inc";

qreg q[5];
creg c[5];

h q[1];
cx q[1],q[0];
measure q[0] -> c[0];
```

Fig. 5: Composer Showing QASM Code

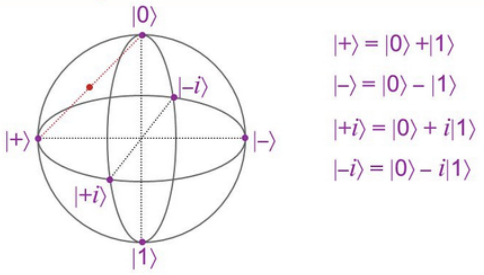


Fig. 6: Bloch Sphere

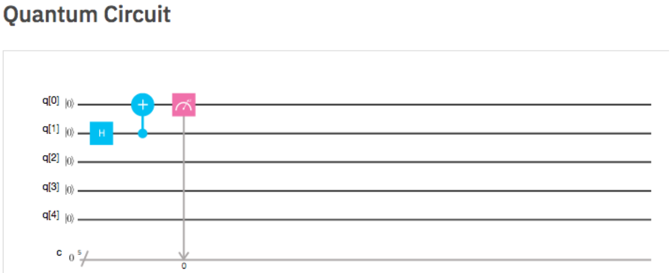


Fig. 7: Superposition Entanglement and Measurement

It must also be noted that, because of the randomness of the quantum process, each instance of the experiment can have different results. The IBM Quantum Experience allows users to specify the number of runs (shots) for an experiment. In this particular experiment, 100 shots were specified. Once completed, the results were displayed as a histogram (fig.8).

This simple simulation was useful in learning to understand how to run a quantum code and prepare for more complicated encryption experiments with the IBM Q Experience Composer.

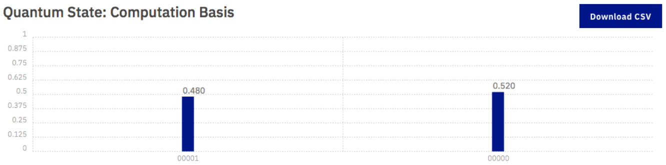


Fig. 8: Quantum State Result

A. Encryption Algorithm Experiment

While quantum encryption is still in a developing state, several studies have already been conducted. Many of them were attempts to lay a foundation for a stable encryption process. Researchers are attempting to develop an encryption model that works on a quantum machine. At this project's onset, several different criteria were examined in order to decide which experiment would be the best for analysis and testing. The biggest concerns were namely the algorithm and the process itself. Many different encryption methods were found throughout the literature. Nonetheless, similarities were found in terms of process and actions taken on the inputI. It was found that, in order to perform quantum encryption, it is necessary to use Quantum gates performing unitary operations, such as polarization and rotation of the qubits. Upon comparison, homomorphic encryption seemed to stand out as the most widely explored type of encryption and the most widely experimented on across the different studies. The main reason for this is that it is a reversible operation which, as a result, makes it possible to verify that the right operation was performed on the input during the encryption simply by looking at the output. Since it is still an emerging field, that is constantly evolving, the date of the publication in relation to current technology was an important factor in choosing the study that would be experimented on. The last and most important aspect that needed to be considered was the capability of testing the algorithm in real-life using the different tools available for this project.

A quantum algorithm developed by researchers from the University of Shanzhou and the University of Science and Technology of China, presented the first encoding algorithm performed on the IBM Quantum Computer. This addressed the concerns of the capability to test the experiment. Similar to most of the other encryption experiments available, this study performs a homomorphic encryption, which is a type of encryption that allows computation on encrypted data [8]. It serves as a scope to show possible future uses and purposes of quantum computers. This encryption generates an encrypted result that, once decrypted, matches the result of the operations performed on the input.

Starting from a quantum algorithm created to solve linear equations proposed by Harrow *et al.* in 2009, the encryption model encodes the problem to test homomorphic encryption [6]. In order to take into account the issue of security, this study presents a different approach by compiling an encrypted version of the input in the first step of the algorithm instead of encoding the quantum circuit on the servers directly. In this case, the server can only deal with encrypted data. After examining the model presented in their study, it became possible to attempt to encode the circuit on IBMs cloud Quantum Computers thanks to the methodology. Among the challenges we faced in our experiment, the most notable was to translate the annotations for the gates and unitary operations presented in the model of the researchers into the corresponding gates and operations available in the IBM Composer following the guidelines of the examined study (Tab. I).

Zhengzhou University Annotation	Transformation (If Applicable)	v	Pace University Annotation
R-Gate R+ Gate (Phase Estimation)	R-Gate-CNOT Gate-R+Gate	v	hadamard gate-CNOT-hadamard Gate
Rotation Ry(θ)	CNOT- Ry(-θ/2) - CNOT Ry(θ/2)	v	CNOT - combination of 7 H gates and 7 T gates - CNOT - Combination of 7 T+ gates and 7 H gates
R-Gate R+ Gate (Inverse Phase Estimation)	R-Gate-CNOT Gate-R+Gate	v	hadamard gate-CNOT-hadamard Gate
Measurement	Measurement	v	Measurement Gate

TABLE I: Annotation Comparisons

To understand the different phases of the algorithm, it is important to fist understand a few concepts, such as the fact that quantum computers only use operations that are their own inverses. As a result, if you apply the operation twice, you will get the same value as the input value. In other words, an operation performed on a qubit can be performed on this qubit the opposite way. In order to write non-reversible functions in a reversible way, quantum computing uses two qubits. One qubit, the input qubit, stays unchanged and the value of the function is written to the output qubit, also called the target qubit. This process makes it possible to rewire operations (fig.9).

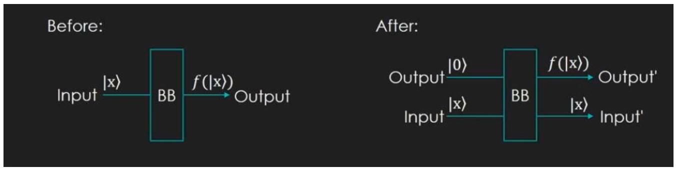


Fig. 9: Reversible Function for Two Circuits

The gates perform operations on qubits. The gates are capable of slightly changing the qubits without collapsing them. In order to understand this concept, one could imagine that the qubits move around the unit circle of a Bloch sphere depending on the operations performed on them. They collapse once they are measured. For example, X gates flip the qubits around the unit circle. An X gate would change the qubit state from 1 to 0. On the other hand, an H gate, also called Hadamard gate, would change the state of 1 or 0 to a flip coin state, which is a state of superposition.

The operations performed by the other gates included in the computation will be examined later in this study. The algorithm studied here uses three qubits. The first qubit is the input qubit. The state of this qubit should not change. The second qubit is a spare qubit. It is needed due to the way quantum circuits work. For instance, we are using the second qubit because CNOT gates operate on pairs of qubits, they cannot operate on a single qubit. This is also represented in the IBM Quantum Composer. The third qubit named in Huangs study, the ancilla operator, is the output qubit. This qubit is the one measured in the new experiment because it was this qubit that got affected by the operations used by the gates. The algorithm would only be successful if the value of the ancilla operator was equal to 1 [8].

The equation in this study can be encoded as the following: $A|x >= |b >$ (1) This equation was considered given the input being $|x >$, the matrix A and the output being vector $|b >$. In order to adapt to quantum requirements, the study considered that $||x|| = ||b|| = 1$.

Huang's algorithm is composed of three different steps. The first step is called the Phase Estimation. It is described in the study as the encryption process. It takes place through the entanglement of the input qubit and the spare qubit. Entanglement occurs by putting the input qubit through the Hadamard gate, which puts it in superposition, and then using a CNOT gate. The input qubit becomes the control qubit and the spare qubit becomes the target qubit. As a result of this process, these two qubits will be in superposition. They will be coordinated, and cannot be separated. Because of the superposition state, their state will be neither 1 or 0. They will have a 50 percent chance to collapse to 0 and a 50 percent chance to collapse to 1. Nonetheless, another Hadamard Gate is added to the input qubit. This other Hadamard gate will change the state of the qubit from superposition back to its original state. As a result of this operation, the two qubits are in the original state of the input qubit. The CNOT gate, that is then operated on the spare qubit, sets the spare qubit as the control qubit and the output qubit as the target qubit. The state of the spare qubit, which is flipped to the output qubit. At this point of the experiment, the output qubit is in the same state as the input qubit. This process takes us back to the fact that quantum computing operations need to be reversible and that the output qubit state should be the same as the input qubit state before operating gates on the output qubit.

The second phase of the experiment is named in Huang's study as the rotation phase. It will operate a succession of Hadamard gates that will change the qubit into a superposition state. Phase gates, called T gates, in the IBM Composer that will rotate the output qubit around the Z axis and T+ gates which are the inverse of the phase gates. The first combination of Hadamard gates and Phase gates will put the qubit into superposition around the different axis of the Bloch sphere before rotating the qubit around the Z axis. The second combination is made of Hadamard gates and T+ gates. This process can be explained as doing the opposite rotation previously done. The goal of this algorithm is showing that the qubit can travel around the Bloch sphere with a high probability for getting an output similar to the input.

The last part of the algorithm is called the inverse phase estimation. This process is described in the model study as the disentanglement of the input qubit and spare qubit, or the decryption process.

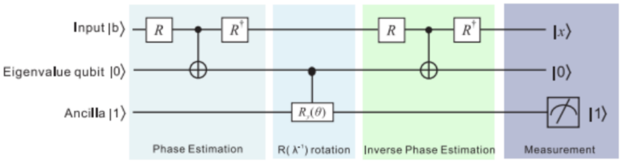


Fig. 10: Huang's Experiment

At first Huang's study was strictly followed, by setting the input qubit as Q(0), the spare qubit as Q(1) and the output qubit as Q(2) (fig. 11). After running the first tests, results were found to be the opposite of those from Huang's study (fig. 12). Further work on the experiment concluded that, in order to perform this algorithm on the IBM Composer, the qubits needed to be flipped to operate the CNOT gates. As a result, Q(0) becomes the output qubit, Q(1) becomes the spare qubit and Q(2) becomes the input qubit. The model in figure 13 shows the final algorithm version executed in our experiment.

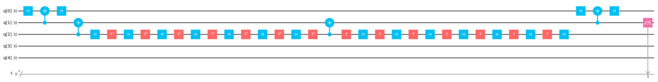
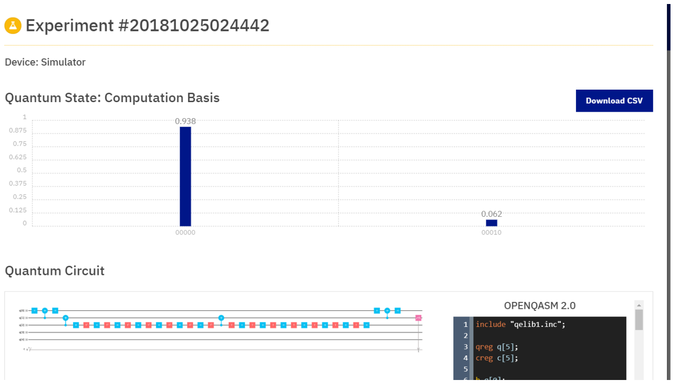


Fig. 11: First Encryption Algorithm IBM Q



Experiment #20181025024442

Device: Simulator

Quantum State: Computation Basis

Quantum Circuit

OPENQASM 2.0

```
include "qelib1.inc";

qreg q[5];
creg c[5];

```

Fig. 12: First Algorithm Results

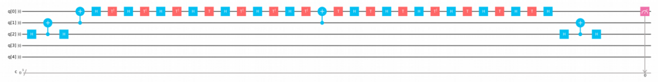


Fig. 13: Final Encryption Algorithm IBM Q

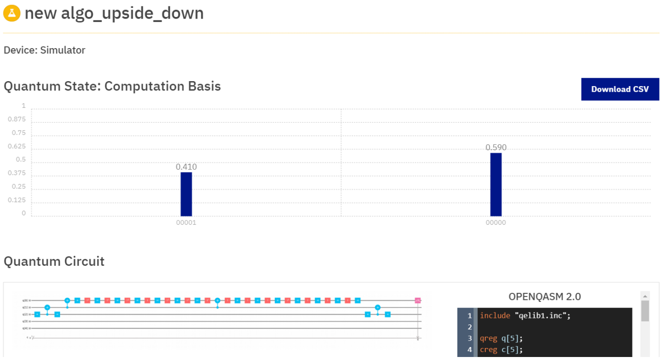
B. Results

Before revealing the results, it is important to understand how the measurements work. The probability calculated is the probability that a qubit collapses to 0 or 1. The measurement gate will fire through 0 and 1 and calculate this probability.

The results of this study, after running the experiment on the real quantum computer and in the simulators, were different from the results of the original study. Some factors and implications needed to be considered in order to draw conclusions from this experiment. For instance, the previous study did not include any details regarding the number of shots executed. When changing the number of shots executed in the new tests the results change. These changes were not significant enough to point to a determining factor. (fig. 12). As shown in the table our results oscillated between 0.400 and 0.500 for the qubit to collapse to 1. It represents a 40 to 50 percent chance for the experiment to get the expected result. These results are far from the results shown in Huang's study. According to their study, the output states were between 0.920 and 0.992. It means that they never fell under a 92 percent chance to get the expected output. The results of our experiment show probabilities that are closer to a superposition state (fig. 14). Furthermore, when measuring the other qubits alone to check if the conditions of the experiment were met, the spare qubit is in the expected state of 1 as it is simply used to conduct the CNOT operations and the input qubit is in a state close to our output qubit due to the last Hadamard gate used in the algorithm, thus proving that the disentanglement process worked.

Results of Huang's Study	Results of Pace University
Between 0.400 and 0.500 for expected result	Between 0.920 and 0.992 for expected result

TABLE II: Results Comparison



new algo_upside_down

Device: Simulator

Quantum State: Computation Basis

```
include "qelib1.inc";

qreg q[5];
creg c[5];
```

Fig. 14: Final Algorithm Results

It is difficult to say that what was discovered is a strong encryption model that can be tested on the IBM Quantum Composer following the provided methodology. It may yet be too early to compute this algorithm using the IBM composer and some recommendations could be made. Indeed, it might be better to test this algorithm using Qsharp (Q), the Microsoft platform for performing Quantum computing simulations. Using this tool would allow one to test inputs while utilizing the same gates as Huang's experiment on the qubits. One limitation of the Microsoft tool is that it only runs simulations and it does not run on a real quantum computer. Also, Huang's experiment uses an eigenvalue in the matrix transformation. This eigenvalue should be passed through the spare qubit in order to be included in the rotation process. This may be possible by using a physical gate called the U2 gate in the IBM Composer. Huangs experiment does not refer to this gate, so it was excluded from this new experiment. One should understand that the goal behind using so many gates is to cover a larger area of the Bloch sphere. Nonetheless, it should also be considered to reduce the number of gates used in the process. By testing with fewer H and T gates the results may differ as the number of operations on the qubits decreases.

V. Conclusion

Quantum cryptography, just like quantum computing, is still very much in the experimental stages with only a handful of actual working machines in existence, and even these have some extreme requirements for operation. Scientists all over the world are busy trying to accomplish any kind of quantum algorithm, let alone one as complex as encryption. Experiments across the literature, agree on the need of operations such as vertical and horizontal polarization in order to achieve what could be a suitable quantum encryption process. However, the application of these experiments have proven to be theoretical, and very difficult to reproduce, rather than scalable proof-of-principle demonstration. Viability may still be a long way off. While the power of quantum computing cannot be denied when it comes to cryptography, the uncertainties around quantum computing, as well as the lack of available tools, remain constant issues in the field, and quantum encryption is no exception. In fact, many tools have to be created solely to complete certain experiments. According to Lindsay, error correction in quantum computing is not as easy as in traditional computing, because random errors in the physical media tend not to be correlated, but correlation, is the whole point of quantum entanglement [11]. When trying to solve simple algorithms, stability in qubits is easy to maintain, however, as the algorithm gets more complex, stability becomes a major issue. Another challenge pointed out by Lindsay, is that some quantum computers actually struggle to maintain coherence long enough to complete useful calculations [11]. Any small disturbances (for example, a small beam of light) can change the direction of the photon even slightly and cause a build up of errors.

While many believe quantum computing will eventually evolve to a point where it will render many common encryption algorithms obsolete, there is still a question as to when. Some theorize that it could be achieved within the next few years, while others believe it will not happen within our generation's lifetime [5]. Regardless if this were to happen or not, it is likely that the entire global internet ecosystem would need to be restructured, as well as human thinking about computing, before the technology could truly be applied [3].

Acknowledgment

The authors would like to thank Prof Charles Tappert, PhD and Prof Avery Leider.

References

[1] "Quantum computing report: Where qubits entangle with commerce," accessed=2018-11-29. [Online]. Available: https://quantumcomputingreport.com/players/universities/

[2] E. Cartlidge, "Europe's 1 billion quantum flagship announces grants," 2018.

[3] S. Chen. Quantum cryptography explained. Youtube. [Online]. Available: https://youtu.be/UiJiXNEm-Go

[4] A. Furuta, "One thing is certain: Heisenberg's uncertainty principle is not dead," *Scientific American*, 2012.

[5] R. Grimes. The quantum break is coming will you be ready? [Online]. Available: https://youtu.be/jB47_xoeB4o

[6] A. W. Harrow, A. Hassidim, and S. Lloyd, "Quantum algorithm for linear systems of equations," *Physical review letters*, vol. 103, no. 15, p. 150502, 2009.

[7] M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," *Reviews of Modern Physics*, vol. 89, no. 1, p. 015004, 2017.

[8] Huang, He-Liang and Zhao, You-Wei and Li, Tan and Li, Feng-Guang and Du, Yu-Tao and Fu, Xiang-Qun and Zhang, Shuo and Wang, Xiang and Bao, Wan-Su, "Homomorphic encryption experiments on ibms cloud quantum computing platform," *Frontiers of Physics*, vol. 12, no. 1, p. 120305, 2017.

[9] Y. Ismail and F. Petruccione, "The race towards quantum security," in *2018 IST-Africa Week Conference (IST-Africa)*. IEEE, 2018, pp. Page–1.

[10] Lai, Hong and Luo, Ming-Xing and Pieprzyk, Josef and Zhang, Jun and Pan, Lei and Li, Shudong and Orgun, Mehmet A, "Fast and simple high-capacity quantum cryptography with error detection," *Scientific reports*, vol. 7, p. 46302, 2017.

[11] J. Lindsay, "Why quantum computing will not destabilize international security: The political logic of cryptology," 2018.

[12] Lo, Hoi-Kwong and Lütkenhaus, Norbert, "Quantum cryptography: from theory to practice," *arXiv preprint quant-ph/0702202*, 2007.

[13] M. Moller and C. Vuik, "On the impact of quantum computing technology on future developments in high-performance scientific computing," *Ethids and Information Technology*, vol. 19, no. 4, pp. 253–269, 2017.

[14] D. Patel, S. Patro, C. Vanarasa, I. Chakrabarty, and A. K. Pati, "Impossibility of cloning of quantum coherence," *arXiv preprint arXiv:1806.05706*, 2018.

[15] J. Prisco. The quantum computing race the us can't afford to lose. Accessed=2018-12-4. [Online]. Available: https://thenextweb.com/contributors/2018/09/01/quantum-race-united-states-must-compete/

[16] A. Segal, N. Nilekani, H. Dixon, M. Flournoy, M. Sulmeyer, V. Mayer-Schiinberger, and T. Ramge, "When china rules the web," *Foreign Affairs*, vol. 97, no. 5, pp. 10–18, 2018.

[17] Y. Wang and K. She, "A practical quantum public-key encryption model," in *Information Management (ICIM), 2017 3rd International Conference on*. IEEE, 2017, pp. 367–372.

[18] C. Woodford, "Quantum computing: A simple introduction," 2012. [Online]. Available: https://www.explainthatstuff.com/quantum-computing.html

[19] L. Xi-Han, L. Chun-Yan, D. Fu-Guo, P. Zhou, L. Yu-Jie, and Z. Hong-Yu, "Quantum secure direct communication with quantum encryption based on pure entangled states," *Chin. Phys. Soc and IOP Publishing LTD*, vol. 16, no. 8, 2007.

[20] Yuan, Yong and Wang, Fei-Yue, "Blockchain: the state of the art and future trends," *Acta Automatica Sinica*, vol. 42, no. 4, pp. 481–494, 2016.