COMP3316 Assignment 4

Fan Zixian 3035771610, Tang Jiaxuan 3036086567, Chen Jingyan 3035827940, Liu Hainuo 3035801685

I. INTRODUCTION

Let's dive into the fascinating world of quantum cryptography, where communication security reaches mind-boggling levels and secrets are hidden behind the mysterious curtain of quantum mechanics. Quantum cryptography, like the super cool BB84 protocol, totally changes the game of information security by using the mind-bending properties of quantum physics to create unbreakable cryptographic keys. This protocol allows people to communicate seamlessly without needing a pre-shared key, even when there are super smart adversaries with crazy computational abilities. Gilles Brassard, a genius in this field, sheds light on the awesome history of quantum cryptography and invites us to explore this mind-boggling world where quantum principles meet the protection of secret information.

II. HISTORY

The annals of quantum cryptography trace back to the early 1960s when visionaries like Stephen Wiesner and Charles Bennett, then young scholars at Brandeis University, delved into the potential of quantum mechanics in cryptography. Wiesner's groundbreaking concepts, from quantum banknotes to multiplexing channels, laid the cornerstone for transformative advancements in the field. As their dialogues evolved into tangible ideas, the stage was set for a pivotal moment in late 1979 when Gilles Brassard's chance encounter in San Juan, Puerto Rico, led to a serendipitous collaboration that birthed innovations like quantum teleportation, entanglement distillation, and the genesis of the BB84 protocol.

The seminal paper on quantum cryptography presented at Crypto '82 marked a watershed moment, introducing the term 'Quantum Cryptography' and catalyzing the resurgence of Wiesner's original work. This historical juncture paved the way for subsequent developments, including the establishment of the lower bound on quantum computer power and the advent of privacy amplification techniques. The transition from theoretical propositions to practical implementations saw pivotal milestones, culminating in the demonstration of the first secret quantum transmission in 1989, affirming the transformative power of quantum mechanics in reshaping information security.

The journey of quantum cryptography unfolds from its prehistory in the early 1960s when Stephen Wiesner and Charles Bennett, then undergraduates at Brandeis University, explored the novel realm of quantum mechanics for cryptographic purposes. Wiesner's pioneering ideas, such as quantum banknotes and multiplexing channels, set the stage for revolutionary advancements in the field. Despite facing rejection in the academic realm due to the technical language barrier, Wiesner's concepts found resonance with Bennett, leading to crucial preservation and eventual dissemination to the scientific community.

In a serendipitous encounter in late October 1979 in San Juan, Puerto Rico, Gilles Brassard, a distinguished figure in quantum cryptography, was introduced to Wiesner's quantum banknotes. This momentous meeting sparked a collaboration that birthed an array of groundbreaking innovations, including quantum teleportation, entanglement distillation, and the inception of the BB84 protocol, a cornerstone in quantum key distribution. The subsequent publication of the first paper on quantum cryptography at Crypto '82 marked a significant milestone, propelling the field into the limelight of cryptographic research.

The elucidation of utilizing quantum properties for secure communication led to the realization of the BB84 protocol, which provided the foundation for secure key distribution through quantum means. The protocol's debut at the 1983 IEEE Symposium on Information Theory marked a turning point in the field, laying the groundwork for the most practical applications in quantum information science. The subsequent demonstration of the first secret quantum transmission in late October 1989—a symbolic decade after the pivotal meeting at the San Juan beach—cemented the achievements in quantum cryptography, illuminating the path for further research and development.

III. MOTIVATION

In today's digital age, keeping our online communications secure is a major concern. We often rely on traditional cryptographic methods, like the RSA protocol, to protect our emails and credit card transactions. But have you ever wondered how secure these methods really are?

Consider the scenario where Eve, a potential eavesdropper, possesses a computer capable of swiftly factoring numbers, potentially compromising the security provided by protocols like RSA. The uncertainty surrounding Eve's computational capabilities poses a significant challenge to maintaining secure communication channels. This leads us to a crucial question: Can we ensure secure communication without relying on assumptions about Eve's computational power?

The answer lies in the realm of quantum cryptography, offering innovative solutions that transcend traditional complexities. One such solution is the one-time pad, a pioneering protocol that offers information-theoretic security. It provides a way to achieve secure communication that doesn't depend on uncertainties in computational capabilities. By exploring protocols such as the BB84 protocol, grounded in the principles of quantum mechanics, we unlock a realm of secure communication where data privacy thrives beyond the limitations of computational assumptions.

IV. THE BB84 PROTOCOL THEORY

A. Mechanism

1. Alice generates $4n$ bits.
2. Alice randomly encodes each bit with computational basis or Fourier basis.
3. Alice sends the encoded qubits to Bob. (Eve can get the result halfway)
4. Bob randomly measures each qubit in computational basis or Fourier basis.
5. Alice and Bob share the chosen bases for each qubit. Then Bob discards any qubits that he measured in a different basis.
6. For each qubit, Bob randomly chooses to either test the consistency of the result with Alice or to use that qubit as the secret key (e.g., map $|0\rangle, |+\rangle$ to bit 1 and map $|1\rangle, |-\rangle$ to bit 0). If the test of consistency fails, it means Eve had measured some of the qubits, and the secure communication fails.

B. Why BB84 is secure

1. If the communication channel is noiseless

Theorem 1 *For any non-orthogonal states $\{|\varphi_0\rangle, |\varphi_1\rangle\}$, one has*

$$\overbrace{\mathcal{C}(|\varphi_i\rangle\langle\varphi_i|) = |\varphi_i\rangle\langle\varphi_i| \otimes \sigma_i}^{\textbf{\textit{No disturbance}}} \implies \overbrace{\sigma_0 = \sigma_1}^{\textbf{\textit{No info.}}} \quad \forall i \in \{0,1\}$$

This theorem is named 'No Information Gain Without Disturbance'. It reveals the fact that any measurement which results no state change is impossible to gain any information.

If the communication channel between Alice and Bob is noiseless, this theorem can thereby be used as a strong argument to show BB84 is secure as Eve should make sure the 'no-disturbance' condition is true.

Therefore, we want to show that

$$\mathrm{Tr}_M \left[U_{AEM}(\rho_A \otimes |\beta\rangle\langle\beta|_{EM}) U^\dagger_{AEM} \right] = \rho_A \otimes \sigma_{iE}$$

is impossible when $\sigma_0 \neq \sigma_1$ where $\rho_A = |\varphi_i\rangle\langle\varphi_i|$ for $\forall i \in \{0,1\}$.

Proof.

Define

$$|\Psi_i\rangle_{AEM} \coloneqq U_{AEM}(|\varphi_i\rangle_A \otimes |\beta\rangle_{EM}) \tag{1}$$

Now

$$\mathrm{Tr}_M \left[|\Psi_i\rangle\langle\Psi_i|_{AEM} \right] = |\varphi_i\rangle\langle\varphi_i|_A \otimes \sigma_{iE} \ \forall i \in \{0,1\} \tag{2}$$

Define

$$\sigma_i \coloneqq |\alpha_i\rangle\langle\alpha_i| \ \ \forall i \in \{0,1\} \tag{3}$$

By equation (2) and (3), we can observe that

$$|\Psi_i\rangle = |\varphi_i\rangle_A \otimes |\alpha_i\rangle_E \otimes |\mu_i\rangle_M \tag{4}$$

Therefore

$$\begin{aligned}&\left(\langle\varphi_0|\otimes\langle\alpha_0|\otimes\langle\mu_0|\right)\left(\langle\varphi_1|\otimes\langle\alpha_1|\otimes\langle\mu_1|\right)\\=&\left(\langle\varphi_0|\otimes\langle\beta|\right)U^{\dagger}_{AEM}U_{AEM}\left(|\varphi_1\rangle\otimes|\beta\rangle\right)\\=&\left(\langle\varphi_0|\otimes\langle\beta|\right)\left(|\varphi_1\rangle\otimes|\beta\rangle\right)\\=&\langle\varphi_0|\varphi_1\rangle\langle\beta|\beta\rangle\\=&\langle\varphi_0|\varphi_1\rangle\end{aligned}\tag{5}$$

Notice that

$$\begin{aligned}&\left(\langle\varphi_0|\otimes\langle\alpha_0|\otimes\langle\mu_0|\right)\left(\langle\varphi_1|\otimes\langle\alpha_1|\otimes\langle\mu_1|\right)\\=&\langle\varphi_0|\varphi_1\rangle\langle\alpha_0|\alpha_1\rangle\langle\mu_0|\mu_1\rangle\end{aligned}\tag{6}$$

Combining (5) and (6), and taking modulus on both sides, we get

$$|\langle\varphi_0|\varphi_1\rangle||\langle\alpha_0|\alpha_1\rangle||\langle\mu_0|\mu_1\rangle| = |\langle\varphi_0|\varphi_1\rangle| \tag{7}$$

Having the fact that $|\langle\mu_0|\mu_1\rangle| \leq 1$, solving (7) gives

$$|\langle\alpha_0|\alpha_1\rangle| \geq 1 \textbf{ or } |\langle\varphi_0|\varphi_1\rangle| = 0 \tag{8}$$

Since $|\alpha_i\rangle$ is a unit vector, we must have $|\langle\alpha_0|\alpha_1\rangle| \leq 1$. In conclusion $|\langle\alpha_0|\alpha_1\rangle| = 1$, it is equivalent to say $|\alpha_0\rangle$ must be in the same state as $|\alpha_1\rangle$ for non-orthogonal states $\{|\varphi_0\rangle, |\varphi_1\rangle\}$. ■

Since we have assumed the communication channel is noiseless, any disturbance made by Eve can be found by Alice and Bob in the step 6 test. Thus, the protocol is secure.

2. If there are noises

Our previous discussions about the security of BB84 is depended on a noiseless communication channel between Alice and Bob. It means that there should not be any error observed by Bob if Eve did not disturb any state. Our assumption is fragile, as the communication channel may not always be noiseless, errors may happen without Eve's disturbance!

The proof become rigorous, but luckily Lo and Chau came up with a solution. The idea is to proof Lo-Chau protocol is secure first, and then show the Lo-Chau protocol is equivalent to BB84 protocol in terms of security.

V. BB84 EXAMPLE

In order to better understand how the BB84 Protocol works, an in detailed example with specific steps is provided following. In this example, Alice tends to send a 8 bits qubit message to Bob through this protocol. Firstly, a tricky point to mention in the quantum communication is that, Alice and Bob has two channels: quantum channel and classical bit channel. The quantum channel is for Alice to send qubit to Bob, and the classical bit channel is for them to go public with their previous choice of basis.

A. Step 1: Alice encodes the message

Initially, Alice have a sequence of bits, which is

$$0\ \ 1\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 1$$

And for each step, Alice and encode this bit in the computational basis and Fourier basis with equal probability $\frac{1}{2}$, represented by + and × respectively. Suppose Alice for encode the sequence with following basis randomly:

$$+\ \ +\ \ \times\ \ +\ \ \times\ \ \times\ \ \times\ \ +$$

Then, we have the encoded sequence:

$$0\ \ 1\ \ |+\rangle\ \ 0\ \ |-\rangle\ \ |+\rangle\ \ |+\rangle\ \ 1$$

B. Step 2: Bob decodes the message

After Bob received Alice's encoded sequence, he will decode the message by randomly choosing the basis. Suppose Bob decodes the sequence with the following basis randomly:

$$+\ \ \times\ \ \times\ \ \times\ \ +\ \ \times\ \ \times\ \ +$$

Then the bits after Bob's measurement is:

$$0\ \ |+\rangle\ \ |+\rangle\ \ |+\rangle\ \ 1\ \ |+\rangle\ \ |+\rangle\ \ 1$$

And after Bob decode the sequence, what he believe is:

$$0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 1$$

C. Step 3: Announcement through classical bit channel

Afterwards, Alice and Bob will announce the bases they used, and discard the bits that they used different bases. Although it is probable that even if they use different basis, the guess from Bob is exactly the same as Alice, to make sure the communication is absolutely correct, they will only consider the bits that they implemented with the same basis. Hence, by the law of large number, expected half of the number of bits will be measured by the same basis, if the N is large. However, in our example, since N is only 8, it is still possible the number is not exactly 4, but it is just to show the probable case in the real world communication. The shared secret key they will finally consider are:

$$0 \;\; discard \;\; 0 \;\; discard \;\; discard \;\; 0 \;\; 0 \;\; 1$$

D. Step 4: Test eavesdropper

Currently we get a sequence of 5, which is about $\frac{1}{2}$ of the original sequence, how are we going to get to the desired $\frac{1}{4}$? This is because of the possible presence of eavesdroppers.

Since Bob and Alice do not know if an eavesdropper exists, but as long as Eve, the eavesdropper, exists, he will definitely measure the intermediate sequence that he overheard, which leads to a probability of $\frac{1}{2}$ to change the final result that Bob receives.

Thus, Bob randomises each bit he receives to determine whether he accepts the bit directly as the key or uses the bit to test for the presence of an eavesdropper, with probability $\frac{1}{2}$. Suppose that out of the 5 bits Bob receives, he takes out 3 to test for the presence of an eavesdropper. Bob will communicate with Alice regarding the value of these 3 bits. If at least one of the value are different, the eavesdropper should exist. Of course, it is also possible that the eavesdropper happens to take the measurements without changing the original result each time, so that the presence of the eavesdropper cannot be detected by this method. However, the likelihood of this being the case in our example is only $\frac{1}{8}$, and can be approximately ignored when N is very large, since the probability of the eavesdropper choosing correctly each time would be exponentially decreasing.

Ultimately, assuming no eavesdropper exists, Alice will complete communication with Bob based on these remained two secret keys. That's where the $\frac{1}{4}$ comes from.

VI. BB84 SIMULATION

In order to show the approximation ratios, a jupyter code is provided for checking. For the details of our code, see our GitHub repository: GitHub link.

A. Suppose no eavesdropper

We define the following functions to complete the simulation process:

```python
def random_bits(n):
    """Generate n random bits."""
def random_bases(n):
    """
    Generate a random sequence of n bases.
    0 represents the computational basis and 1
        represents the Fourier basis.
    """
def encode_bits(bits, bases):
    """
    Encode bits based on the selected bases.
    Z basis (0) does not change the bit; X basis
         (1) encodes 0 as |+> and 1 as |->.
    """
def measure_bits(encoded, bob_bases):
    """
    Bob measures the encoded bits based on his
        choice of bases.
    If the bases match, he gets the correct bit.
    """
def extract_key(bits, bases, bob_bases):
    """
    Extract the shared key from bits where the
        bases match.
    """
def bb84_simulation(n_bits)

n_bits = 4096
alice_key, bob_key = bb84_simulation(n_bits)
print("Length: ", len(alice_key))
```

Listing 1: Python simulation (No eavesdropper)

We set Alice's sequence to have 4096 bits at the beginning. And we obtained length 2023 of the matched sequence, which is about 1/2, which meets expectations.

B. Suppose eavesdropper exists

Then Alice and Bob will randomly announce some the keys to compare. Suppose we still have the original sequence length 4096, and we have the following code to test.

```python
def eve_intercept_measure(encoded, bases):
    """Simulate Eve intercepting and measuring
        the quantum bits."""
def compare_keys(alice_key, bob_key):
    """Randomly compare parts of the keys to
        detect eavesdropping."""
def bb84_with_eavesdropping(n_bits)

n_bits = 4096
alice_key, bob_key, matches, total_compared =
    bb84_with_eavesdropping(n_bits)
print(f"Matching keys in sample: {matches}/{
    total_compared}")
```

Listing 2: Python simulation (With eavesdropper)

For example, at one time we had a result of $\frac{549}{1063}$, which means that Alice and Bob will draw another 1063 bits from the matched sequence for eavesdropper detection. It indicates that just $\frac{1}{4}$ of the remaining sequence is used for communication. And if the eavesdropper exists, since there is only a 50% probability that his measurements for each bit do not affect the original result, he has no effect on only 549 of those 1063. And since Alice and Bob only need to find at least one difference in these 1063 to prove that the eavesdropper exists, it is clear that the eavesdropper exists in the current situation.

VII. MORE QKD PROTOCOLS

In addition to BB84, there are other quantum key distribution (QKD) protocols, each with different characteristics and applicable scenarios. Here are some common QKD protocols:

1. E91 protocol

The E91 protocol is based on the EPR entanglement pair, so we also call it the EPR protocol, and its security is guaranteed by the Bell theorem. The implementation of E91 protocol includes two operations of information transmission and information security detection. In E91 protocol, the security of the channel is detected by the Bell inequality. If the detection results of the communication parties do not violate the Bell inequality, it proves that EVE exists. If the detection results of the communication parties do not meet the Bell inequality, it means that there is no EVE in the information transmission channel. Compared with BB84, the E91 protocol simplifies the key distribution process to a certain extent, but it also requires higher resources and technology.

2. B92 protocol

B92 protocol is a simplification of BB84 protocol. The implementation of the protocol is based on two non-orthogonal quantum bits, due to the non-orthogonality of the adopted quantum bits satisfies the quantum unclonability theorem, so that the attacker can not obtain the valid information of the quantum key from the protocol. The B92 protocol is relatively weak and vulnerable to specific attack methods.

3. SARG04 protocol The SARG04 protocol is a simplified form of BB84 that encodes the key using just one non-orthogonal state, it uses weak laser pulses and a decoy-state technique. The protocol is easy to implement and secure against photon number splitting attacks.

VIII. SUMMARY

In the above Note, we described the historical origins of BB84 and the necessary motivation to study it. Immediately after that BB84's theories and proofs are provided for reference. Then we give an example to apply BB84 and prove the correctness of the approximation ratio. Finally, we mention some other protocols as extensions of BB84, which the reader can study on his own if interested.

[1] Brassard, G. (2005). Brief history of quantum cryptography: A personal perspective. *Proceedings of IEEE Information Theory Workshop on Theory and Practice in Information Theoretic Security.* https://doi.org/10.1109/itwtpi.2005.1543949

[2] Shor, P. W., & Preskill, J. (2000). Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters, 85*(2), 441–444. https://doi.org/10.1103/physrevlett.85.441

[3] Chiribella, G. (2024). Chapter 21: Secure communication. In *Quantum Information.* https://moodle.hku.hk/course

[4] Scarani, V., Acin, A., Ribordy, G., & Gisin, N. (2004). Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulses implementations. *Physical Review Letters, 92*(057901). https://doi.org/10.1103/PhysRevLett.92.057901