European IT Certification Curriculum
Self-Learning Preparatory Materials

EITC/IS/QCF

Quantum Cryptography Fundamentals

This document constitutes European IT Certification curriculum self-learning preparatory material for the EITC/IS/QCF Quantum Cryptography Fundamentals programme.

This self-learning preparatory material covers requirements of the corresponding EITC certification programme examination. It is intended to facilitate certification programme's participant learning and preparation towards the EITC/IS/QCF Quantum Cryptography Fundamentals programme examination. The knowledge contained within the material is sufficient to pass the corresponding EITC certification examination in regard to relevant curriculum parts. The document specifies the knowledge and skills that participants of the EITC/IS/QCF Quantum Cryptography Fundamentals certification programme should have in order to attain the corresponding EITC certificate.

Disclaimer

This document has been automatically generated and published based on the most recent updates of the EITC/IS/QCF Quantum Cryptography Fundamentals certification programme curriculum as published on its relevant webpage, accessible at:

https://eitca.org/certification/eitc-is-qcf-quantum-cryptography-fundamentals/

As such, despite every effort to make it complete and corresponding with the current EITC curriculum it may contain inaccuracies and incomplete sections, subject to ongoing updates and corrections directly on the EITC webpage. No warranty is given by EITCI as a publisher in regard to completeness of the information contained within the document and neither shall EITCI be responsible or liable for any errors, omissions, inaccuracies, losses or damages whatsoever arising by virtue of such information or any instructions or advice contained within this publication. Changes in the document may be made by EITCI at its own discretion and at any time without notice, to maintain relevance of the self-learning material with the most current EITC curriculum. The self-learning preparatory material is provided by EITCI free of charge and does not constitute the paid certification service, the costs of which cover examination, certification and verification procedures, as well as related infrastructures.

TABLE OF CONTENTS

EITC/IS/QCF QUANTUM CRYPTOGRAPHY FUNDAMENTALS DIDACTIC MATERIALS
LESSON: INTRODUCTION
TOPIC: INTRODUCTION TO QUANTUM KEY DISTRIBUTION

Welcome to this didactic material on the fundamentals of Quantum Cryptography, specifically Quantum Key Distribution (QKD). This material aims to provide a comprehensive understanding of QKD protocols and their security.

In order to grasp the security aspects of QKD, it is essential to first understand how these protocols work. We will examine each stage of the protocol in detail to gain insight into the underlying physical and quantum mechanical phenomena that ensure the security of the protocol, regardless of the adversary's computational power.

Throughout this material, we will encounter various mathematical concepts and theorems, such as quantum states, measurements, the no-cloning theorem, and entropy. These concepts play a crucial role in the analysis and proof of security for QKD protocols.

To begin, we will explore classical cryptography, which has a long history dating back to ancient times. We will discuss the limitations of classical encryption schemes and the requirements for secure message encryption and decryption. This will motivate the introduction of quantum mechanics into cryptography.

Next, we will delve into the workings of QKD by studying a specific example known as the BB84 protocol. This protocol, proposed in 1984, was the first QKD protocol and serves as an excellent illustration of the different stages involved in QKD. Studying the BB84 protocol will provide a concise summary of the topics covered in the upcoming sections.

Now, let's shift our focus to classical cryptography and explore the Caesar cipher. This encryption scheme involves shifting each letter of the alphabet by a fixed number of positions. We will use the example of a three-step shift, where 'A' becomes 'D', 'B' becomes 'E', and so on. This simple encryption scheme was historically used by the Romans for military communication.

Suppose we want to send a message using the Caesar cipher, such as "We are meeting at the apple tree." We encrypt each letter according to the three-step shift, resulting in the ciphertext: "Zh duh phdw lq wkh dssoh whhu."

While the ciphertext may appear unreadable to unintended recipients, it is not entirely secure. The frequency distribution of letters in a language can be exploited to decrypt such messages. For example, in the English language, the letter 'E' is the most frequently used. By analyzing the frequency of letters in the ciphertext, one can make educated guesses about the corresponding plaintext letters.

This didactic material has introduced the fundamentals of Quantum Cryptography, focusing on Quantum Key Distribution protocols. We have explored the motivations behind using quantum mechanics in cryptography and examined the workings of classical encryption schemes like the Caesar cipher. This material sets the stage for further discussions on QKD protocols and their security.

In the field of cybersecurity, one of the fundamental concepts is quantum cryptography, specifically quantum key distribution. This form of cryptography aims to provide secure communication between two parties, often referred to as Alice and Bob.

Traditional encryption schemes, such as those based on frequency analysis or letter shuffling, are vulnerable to decryption. However, there are encryption schemes that are provably secure, one of which is the one-time pad.

The one-time pad encryption scheme involves the use of keys by Alice and Bob. These keys are bit strings that are used for encryption and decryption. The process begins with Alice encrypting her message, represented as a bit string, using her key. This encryption is done through binary addition, where different bits result in a 1 and the same bits result in a 0.

Once the message is encrypted, Alice sends the ciphertext, represented as another bit string, to Bob over a

public channel. This channel is accessible to anyone, including potential adversaries. However, the security of the encryption lies in the fact that the ciphertext reveals no information about the original message.

Upon receiving the ciphertext, Bob decrypts it using his key through binary addition. The result of this decryption is the original message that Alice intended to send. It is important to note that this encryption scheme assumes that Alice and Bob have perfectly matching keys.

To illustrate this process, let's consider an example. Suppose Alice wants to send the message "0110100" as a bit string. Using her key "1011101", she performs binary addition, resulting in the ciphertext "1101001". Bob, who possesses the same key as Alice, decrypts the ciphertext using binary addition and obtains the original message "0110100".

This encryption scheme is provably secure, meaning that it offers information-theoretic security. This implies that even though the ciphertext is transmitted over a public channel, an adversary cannot gain any information about the original message.

It is important to acknowledge that this idealized scheme assumes no errors or losses in transmission. In reality, these factors need to be considered. However, for the purpose of understanding the concept, we can focus on the ideal scenario where Bob receives the exact message that Alice intended to send.

Quantum key distribution, specifically the one-time pad encryption scheme, provides provable security in communication. By utilizing bit strings as keys and performing binary addition, Alice and Bob can securely exchange messages without the risk of adversaries gaining any information.

Quantum Key Distribution (QKD) is a fundamental concept in the field of cybersecurity. It provides a secure method for generating and sharing encryption keys between two parties, Alice and Bob, using the principles of quantum mechanics. In order to understand QKD, we need to first understand the requirements for a secure encryption key.

The key used in QKD must fulfill several criteria. Firstly, it needs to be truly random, meaning that the bit strings used by Alice and Bob must be sequences of truly random bits. Secondly, the key needs to be at least as long as the message being transmitted. This ensures that the key is not used multiple times, which could potentially compromise the security of the communication. Thirdly, the key should never be used in its entirety or even partially, as this could leak information about the messages being sent. Lastly, the key must be kept completely secret, with no information about it being given to any potential adversaries.

If these four requirements are met, the encryption scheme used in QKD, known as the one-time pad, is provably secure. This means that the communication between Alice and Bob can be conducted without the fear of interception or the compromise of their secrets.

However, creating a truly random and secret key is not a trivial task. Alice and Bob cannot simply meet and agree on a key, as this would allow them to share the messages they want to send. Instead, a device called the ideal key generator is needed. This device generates keys for Alice and Bob while taking into account the possibility of interception by an adversary, whom we will refer to as Eve.

The ideal key generator involves three parties: Alice, Bob, and Eve. It outputs keys, si, for Alice and sk for Bob. However, if it detects that Eve is interfering too much during the key generation process and obtaining too much information about the key, it aborts the process. The ideal key generator needs to meet certain requirements. Firstly, the keys it generates must be correct, meaning that Alice and Bob hold the same bit string as their keys. Secondly, the key must be close to perfect, meaning that Eve has no knowledge of the key and that the individual key bits are uncorrelated.

To achieve these requirements, quantum mechanics comes into play. In QKD, bits are encrypted into quantum states using the polarization of photons. Linear polarization, where the oscillation of photons occurs in one direction, is used in QKD. Two different bases are used: the rectilinear basis (horizontal and vertical) and the diagonal basis (45-degree and 135-degree angles). By encoding bits into these different bases, Alice can send quantum states to Bob, who can then measure them using compatible bases.

The specific QKD protocol, known as DBA T, involves seven steps. However, before diving into the protocol, it is

important to understand how bits can be encrypted into quantum states using photon polarization.

QKD is a secure method for generating and sharing encryption keys using the principles of quantum mechanics. It ensures that the keys are truly random, as long as the message being transmitted, and kept secret from potential adversaries. The use of quantum states and photon polarization allows for the encryption of bits in a secure manner.

In quantum cryptography, one of the fundamental concepts is quantum key distribution (QKD). QKD allows two parties, Alice and Bob, to communicate and create a secret key that can be used for encryption. The protocol involves the use of quantum states and classical channels.

To understand QKD, it is important to first understand the concept of polarization. Photons can be polarized in different ways, such as vertically or horizontally. There are also diagonal bases, where photons are polarized at 45 degrees or minus 45 degrees. To distinguish between these different polarization states, polarization filters can be used. When a vertically polarized photon passes through a filter, it is deflected to the right, while a horizontally polarized photon is deflected to the left.

However, when a photon encoded in the diagonal basis passes through a filter intended for rectilinear basis photons, the polarization of the photon changes. It can become horizontally or vertically polarized, with equal probability. This means that when a photon encoded in the diagonal basis passes through such a filter, all information about its original polarization is lost.

Now, let's move on to the QKD protocol. The first step is to fix the encoding of the bits. For each bit, Alice and Bob choose which polarization state corresponds to the bit. The basic setup involves Alice and Bob wanting to create a secret key. They have access to a quantum channel, where they can send quantum states, and a classical channel, where they can send classical messages.

There is also an adversary, Eve, who can access the quantum channel and listen to the classical channel. However, she is not allowed to change the messages on the classical channel. The goal of the protocol is to ensure that Alice and Bob can create a secret key without Eve being able to intercept or tamper with the communication.

The protocol begins with Alice choosing a random bit string and randomly choosing an encoding basis for each bit. She uses these bases to encrypt the bits, resulting in photons in different states. These photons are then sent to Bob, who also randomly chooses decoding bases to decode the states Alice has sent. Bob receives a bit string, which may not be equal to Alice's bit string due to the choice of bases.

To generate a key, Alice and Bob compare the bases they have chosen. If they have chosen the same basis for a bit, they have the same bit as a result. If they have chosen different bases, that bit is discarded. They then check for any eavesdropping by comparing a subset of the shared information. If there has been no eavesdropping, they can proceed to generate a key.

Quantum key distribution is a protocol that allows two parties to create a secret key using quantum states and classical channels. The protocol involves encoding and sending photons, choosing bases, comparing bits, and checking for eavesdropping. By following this protocol, Alice and Bob can establish a secure key for encryption.

In the field of cybersecurity, a promising approach to secure communication is quantum cryptography. Quantum key distribution (QKD) is a fundamental concept in quantum cryptography that allows two parties, Alice and Bob, to establish a secret key that can be used for secure communication.

The basic idea behind QKD is to exploit the principles of quantum mechanics to detect any eavesdropping attempts. The protocol starts with Alice generating a random bit string and encoding it into quantum bits, or qubits. She then sends these qubits to Bob through a quantum channel.

To ensure the security of the key, Alice and Bob need to perform a series of steps. First, Bob randomly chooses a basis to measure the qubits he receives. After the measurement, Bob reveals his choice of basis to Alice over a classical public channel. Alice compares Bob's basis with her own and discloses the bits they measured in the same basis.

If there was no eavesdropping, Alice and Bob will find that they share the same random bit string. However, if an eavesdropper, Eve, intercepts their communication, she may try to measure the qubits and gain information about the key.

In the case of interception, Eve needs to randomly choose a basis for measurement. If she chooses the wrong basis, she will obtain a random result. However, if she chooses the correct basis, she will obtain the bit value that was encoded by Alice.

To detect eavesdropping, Bob needs to reveal some of the resulting bits to Alice. If they find discrepancies in their measurements, they can conclude that eavesdropping has occurred. Bob needs to reveal enough bits for Alice to estimate the amount of information that Eve has obtained. Based on this estimation, they can decide whether to continue with the protocol or abort it.

After the QKD protocol, Alice and Bob perform two classical post-processing steps: error correction and information reconciliation. Error correction ensures that the bit strings held by Alice and Bob are identical, even if Eve has some knowledge about them. Information reconciliation minimizes the knowledge that Eve has about the bit string.

It is important to note that QKD protocols, such as the one described here, have security proofs, meaning they are provably secure against certain types of attacks.

In the next part of this series, we will delve into the mathematical concepts necessary to describe quantum key distribution protocols. We will explore quantum channels, measurements, and theorems that play a crucial role in analyzing the security of these protocols.

EITC/IS/QCF QUANTUM CRYPTOGRAPHY FUNDAMENTALS DIDACTIC MATERIALS
LESSON: QUANTUM INFORMATION CARRIERS
TOPIC: QUANTUM SYSTEMS

In this didactic material, we will discuss the fundamentals of quantum cryptography, specifically focusing on quantum information carriers and quantum systems. Quantum key distribution is a protocol used to ensure secure communication between two parties, Alice and Bob. To understand this protocol, we need to develop a mathematical description of the physical systems and processes involved.

The protocol consists of three stages: preparation, channel, and measurement. In the preparation stage, Alice prepares the quantum states that she wants to send to Bob. These states are described using density operators, which are elements of the operators over the Hilbert space (denoted as H). A Hilbert space is a vector space over the complex numbers and has a scalar product. An orthonormal basis of a Hilbert space is a family of vectors that satisfy certain conditions.

The channel stage involves the transmission of the prepared states from Alice to Bob. This stage includes any attacks performed by Eve, losses in the channel, and noise from the environment. All these factors are incorporated into the channel description.

The measurement stage is where Bob measures the states he receives from Alice and obtains classical outcomes. The measurement results are crucial for establishing a secure key.

Density operators play a significant role in quantum cryptography as they represent the most general formalism that includes both pure states and mixed states. A density operator, denoted as ρ, is a Hermitian operator that maps from the Hilbert space to itself. It must be normalized, Hermitian, and positive semi-definite. It can also be viewed as an ensemble of pure states, where each pure state is assigned a probability. The identity operator is given by the sum of the probabilities multiplied by the corresponding ket-bras.

Qubits are essential in quantum key distribution as they are used to encode information. Mathematically, qubits can be represented as the zero and one vectors, corresponding to horizontally and vertically polarized states of a photon. A general qubit state is a linear combination of the zero and one vectors with probability amplitudes α and β.

The security of quantum key distribution relies on the mathematical descriptions of the preparation, channel, and measurement stages. Density operators are used to describe the prepared states, and qubits are the quantum information carriers. Understanding these fundamental concepts is crucial for implementing and analyzing quantum cryptographic protocols.

In the field of quantum cryptography, understanding the fundamentals of quantum information carriers is crucial. Quantum systems rely on complex numbers that fulfill the condition that the absolute value squared sums to one. The amplitudes, denoted as alpha and beta, represent the quantum information carriers, while the probabilities are given by the absolute value squared. It is important to note that the sum of the absolute value squared must equal one.

In quantum systems, basis vectors are used to represent the information carriers. The computational basis, for example, consists of the zero vector and the one vector. Another common choice is the Hadamard basis, denoted as the plus and minus vectors. These basis vectors form an orthonormal basis for the qubit state space and correspond to diagonal polarization in the BB84 protocol.

Moving on to the next stage, the quantum channels, we need to understand what a quantum channel is. Mathematically, a quantum channel is a linear, completely positive, and trace-preserving map denoted as a curly symbol. It maps operators from the first Hilbert space, denoted as Ha, to operators in the second Hilbert space, denoted as Hb.

Let's break down the adjectives used to describe a quantum channel. Firstly, a quantum channel is linear, meaning it satisfies the equation for a linear combination of states. Secondly, it is completely positive, which means that the map applied to a state must be positive semi-definite for all positive semi-definite states. Lastly, a quantum channel is trace-preserving, ensuring that the trace of the quantum state remains unchanged after

applying the channel.

To further understand quantum channels, we can use the Kraus decomposition. This allows us to write the map as a sum over operators, denoted as K, applied to the input state. The operators K capture the behavior of the quantum channel.

Understanding the fundamentals of quantum information carriers and quantum systems is essential in the field of quantum cryptography. Quantum channels play a crucial role in the transmission of quantum states, and they are characterized as linear, completely positive, and trace-preserving maps. The Kraus decomposition provides a way to represent quantum channels as a sum over operators.

In the field of quantum cryptography, it is essential to understand the fundamentals of quantum information carriers and quantum systems. One crucial aspect is the concept of operators. Operators, denoted as KJ, are maps from the Hilbert space HA to the Hilbert space HB. In the context of quantum cryptography, these operators are used to describe the behavior of the quantum channel. Specifically, they are used to describe the scrambling channel, which is responsible for the transmission of quantum information.

There are certain conditions that these operators must fulfill. Firstly, there are D operators to describe the scrambling channel, where D is the product of the dimensions of the Hilbert spaces involved. Additionally, if you sum the adjoint of the operators (KJ dagger) multiplied by the original operators (KJ), the result must be the identity operator. This condition ensures that the operators preserve the information being transmitted.

A theorem states that if you have a linear, completely positive, and trace-preserving map, you can always find a Kraus decomposition for this map. Conversely, if you have a map that has a Kraus decomposition, then it is linear, completely positive, and trace-preserving. These descriptions are equivalent and provide a mathematical framework for understanding the behavior of the quantum channel.

To illustrate the concept of channels, let's consider an example of a unitary evolution. This evolution describes the behavior of a closed system. In this case, there is only one operator, denoted as U, which represents the unitary transformation applied to the initial state to obtain the resulting state. Unitary evolutions are always reversible, and finding the inverse of the unitary evolution is straightforward by taking the adjoint of the map.

However, when dealing with open systems, the evolution is more complex. One example is the amplitude damping channel. This channel describes the decay of a two-level system, such as an atom. If the atom is in its excited state, it will transition to the ground state with a probability gamma, where gamma is between 0 and 1. Conversely, the atom will stay in its excited state with a probability of 1 minus gamma. If the atom is already in its ground state, it will remain in that state with a probability of 1.

The operators for this type of channel are K1 and K2. K1 is described as the square root of gamma times the ket row, while K2 is described as the ket row plus the square root of 1 minus gamma times the ket prov 1. These operators ensure that the probabilities of transitioning between states are correctly modeled, and their sum satisfies the condition for the scrambling channel.

In the context of quantum cryptography, it is also important to consider measurements. Measurements are mathematically described by positive operator-valued measures (POVMs). A POVM is a collection of operators that fulfills certain conditions. Each operator in the collection corresponds to a specific outcome, and these operators are positive. Moreover, the sum of all the operators in the collection is equal to the identity operator.

To calculate the probability of obtaining a specific outcome from the measurement, we take the trace of the product of the state and the corresponding operator. For a pure state, this simplifies to sandwiching the state between the operator. Additionally, we can compute the expectation value of the POVM by summing the outcomes multiplied by the trace of the state times the corresponding operator.

As an example, let's consider measuring qubits in the computational basis. If we have a qubit in the state rho, which is described by the density matrix created with the pure states $|0\rangle$ and $|1\rangle$, we can use a POVM to measure the qubit in the computational basis.

Understanding the concepts of operators, channels, and measurements is crucial in the field of quantum cryptography. These concepts provide the mathematical framework for analyzing and modeling the behavior of

quantum information carriers and quantum systems.

In the field of cybersecurity, quantum cryptography is a fundamental concept that relies on the principles of quantum information carriers and quantum systems. Quantum information carriers are represented by qubits, which can exist in a superposition of states, such as 0 and 1. The operators associated with these states are known as PI 0 and PI 1, which are ket-bra operators representing the states of zeros and ones, respectively. It is important to note that the sum of these operators is equal to 1, as required for a valid probability distribution.

When it comes to computing probabilities in quantum cryptography, the trace over the state row multiplied by the POV (Positive Operator Valued) operator is used. For instance, to calculate the probability of obtaining an outcome of 0, the trace of the state row multiplied by the POV operator PI 0 is taken. In the case of a pure state, the calculation can be simplified using the sandwich method, where the pure states are placed outside of the POV element. By performing these calculations, it becomes evident that the probability of obtaining a 0 outcome is equal to the absolute value of alpha squared, while the probability of obtaining a 1 outcome is equal to the absolute value of beta squared.

However, what happens when the measurement is conducted in a different basis, such as the Hadamard basis? In this case, the POV operators, PI plus and PI minus, are used. These operators are similar to the previous ones, but they are defined in terms of the Hadamard basis. By calculating the probability of obtaining a plus outcome in the computational basis, it is found that the probability is equal to the absolute value of alpha plus beta squared divided by 2. This differs from the previous outcome, indicating that the probabilities obtained depend on the type of measurement basis chosen.

It is worth noting that the choice of measurement basis is crucial in quantum cryptography. The probabilities obtained during measurements depend on the basis chosen, even if the plus/minus basis is considered as valid as the 0/1 basis for describing qubits. This has been demonstrated in previous videos, where measuring a qubit in the wrong basis resulted in random outcomes. The mathematical reasoning behind this phenomenon lies in the dependence of probabilities on the measurement basis.

To summarize, the preparation, channel, and measurement stages of quantum key distribution protocols can be mathematically described using density matrices, completely positive and trace-preserving linear maps, and positive operator-valued measures, respectively. These mathematical descriptions are essential for analyzing the security of quantum key distribution protocols. In the next session, we will explore the no-cloning theorem, which plays a crucial role in ensuring the security of these protocols.

Quantum Cryptography Fundamentals - Quantum Information Carriers - Quantum Systems

In the field of quantum cryptography, it is crucial to understand the concept of quantum information carriers and quantum systems. These fundamental aspects play a significant role in ensuring secure communication and protecting sensitive data from potential adversaries.

One key concept in quantum cryptography is the use of quantum states as information carriers. Quantum states are unique configurations of quantum systems that can be manipulated and measured to encode and transmit information securely. By exploiting the principles of quantum mechanics, quantum states can provide an unprecedented level of security in communication protocols.

An essential property to consider when discussing quantum cryptography is entropy. Entropy is a measure of the uncertainty or randomness associated with a system. In the context of quantum key distribution protocols, entropy plays a vital role in the security analysis. Theorems and properties related to entropy are extensively used in analyzing the security of quantum key distribution protocols.

Understanding the principles of quantum information carriers and quantum systems is crucial for comprehending the foundations of quantum cryptography. By harnessing the unique properties of quantum states, secure communication can be achieved, ensuring that information remains confidential and protected from unauthorized access.

Thank you for your attention, and we hope you found this material informative. Stay tuned for more exciting insights into the fascinating world of quantum cryptography.

EITC/IS/QCF QUANTUM CRYPTOGRAPHY FUNDAMENTALS DIDACTIC MATERIALS
LESSON: QUANTUM INFORMATION CARRIERS
TOPIC: COMPOSITE QUANTUM SYSTEMS

In this didactic material, we will discuss the fundamentals of quantum cryptography, specifically focusing on composite quantum systems and the mathematical description of such systems. Before we delve into the topic of entropy, it is essential to understand composite systems, which involve a Hilbert space that is a tensor product of Hilbert spaces.

Composite systems arise when two independent quantum experiments take place simultaneously. For instance, Alice and Bob each have their own labs where they prepare quantum states, send them through quantum channels, and perform measurements. Although these experiments are independent and do not influence each other, we can still view them as one system.

To mathematically describe composite systems, we use tensor products of states, quantum channels, and measurements. For example, the state of the composite system is denoted as Rho_A ⊗ Rho_B, where Rho_A represents the state prepared by Alice and Rho_B represents the state prepared by Bob. Similarly, the quantum channel applied to the composite system is denoted as E_A ⊗ E_B, and the measurement performed is denoted as M_A ⊗ M_B.

It is important to note that composite systems are not limited to two parties like Alice and Bob; they can involve multiple parties, resulting in a tensor product of multiple Hilbert spaces. Most of the concepts discussed in this material apply to multi-partite Hilbert spaces as well.

When considering the basis of a tensor product Hilbert space, we start with the basis states of the subsystem Hilbert spaces. For example, the basis of Hilbert space H_A is denoted as |C_i⟩, and the basis of Hilbert space H_B is denoted as |F_j⟩. The basis of the tensor product Hilbert space is then constructed by taking every possible combination of |C_i⟩ and |F_j⟩. This leads to a formula for the dimension of the tensor product Hilbert space, which is the product of the dimensions of the subsystem Hilbert spaces.

In terms of notation, we can simplify the expression of tensor products by omitting the tensor product symbol. When two ket vectors are written next to each other, it implies a tensor product. Additionally, we can use subscripts on the vectors to indicate which system they belong to. For example, |E⟩_A represents a ket vector belonging to system A, and |E⟩_B represents a ket vector belonging to system B.

Understanding composite quantum systems is crucial for comprehending the security of quantum key distribution. By mathematically describing these systems using tensor products, we can analyze the states, quantum channels, and measurements involved. Composite systems can involve multiple parties, and the basis of the tensor product Hilbert space is constructed by combining the basis states of the subsystem Hilbert spaces.

In the field of quantum cryptography, understanding the fundamentals of quantum information carriers is crucial. One important concept to grasp is composite quantum systems. In the previous material, we discussed qubits, but in reality, we are often dealing with systems of multiple qubits. Let's explore the example of a composite system with two qubits.

In a one-qubit space, we have the computational basis, denoted by states 0 and 1. The vector representation of these states is [1 0] and [0 1], respectively. When we have a system of two qubits, we can assign a computational basis to each subsystem. The basis of the composite Hilbert space is then given by the tensor product of the one-qubit basis. This means we take every possible combination of the zeros and ones to obtain the basis of the two-qubit space. As a result, we now have four basis states, which aligns with the dimension formula we discussed earlier. The dimension of the one-qubit space is 2, and when we have two of these spaces, the dimension of the two-qubit space becomes 4.

To represent the vector of the two-qubit space, we can take the algebraic tensor product of the one-qubit basis vectors. This results in a four-dimensional vector, with the one in the upper place. By following this approach, we can calculate the vector representation of each basis state, such as the state 0 0. These vectors form the basis for the two-qubit space.

Now, let's consider a general two-qubit state, denoted as psi. This state is a linear combination of the four basis states we discussed earlier, with coefficients alpha, beta, gamma, and delta. We can represent this state as a vector with four entries, corresponding to the coefficients in the linear combination. It's important to note that these coefficients must fulfill a normalization condition to ensure that psi represents a physical state.

Up until now, we have focused on product states, where the individual qubits can be determined with certainty. However, there's more to composite systems than just product states. Let's consider a situation where we have a tensor product of zero states in Alice's system and one states in Bob's system. In this composite state, we have a superposition of states, making it challenging to determine the states of the individual qubits. This state is known as the V plus state.

This brings us to the concept of entanglement. If a pure bipartite state, represented by psi, cannot be written as a product state, it is considered entangled. In other words, there are no states phi a and phi b that, when tensor producted, give the state psi. To determine if a given state is entangled, we can use the Schmidt decomposition. This theorem states that any pure bipartite state psi can be written as a sum over coefficients lambda i and the tensor product of basis states in Alice's and Bob's systems. The sum is taken over i from 1 to the Schmidt rank, denoted as d. The coefficients lambda i must be strictly positive, and the squares of lambda i must sum up to 1.

Understanding composite quantum systems and the concept of entanglement is essential in the field of quantum cryptography. By studying the tensor product of basis states and utilizing the Schmidt decomposition, we can gain insights into the behavior of quantum information carriers.

In the field of quantum cryptography, understanding the fundamentals of quantum information carriers is crucial. One concept that plays a significant role in this area is the composite quantum system. When considering a composite quantum system, we often encounter the term "Schmidt decomposition." This decomposition allows us to express the state of a composite quantum system as a combination of subsystems.

The Schmidt decomposition tells us that the dimension of the composite system, denoted as "d," is always less than or equal to the minimum dimension of the subsystems involved. In other words, if we have a qubit system (a two-dimensional system) combined with a larger system of dimension 1 billion, we can always find a subspace in the larger system that includes only the relevant information for our analysis.

Furthermore, the Schmidt decomposition provides insights into the entanglement of a state. If a state is entangled, the Schmidt rank, denoted as "T," is always strictly greater than 1. By calculating the Schmidt rank through the Schmidt decomposition, we can determine whether a state is entangled or a product state.

Let's consider an example to illustrate this concept. Suppose we have the state "Phi plus," which is known to be entangled. By examining its Schmidt decomposition, we can determine its Schmidt rank, which is 2. This confirms that "Phi plus" is indeed an entangled state.

It's important to note that the Schmidt decomposition is applicable only to bipartite states, where we divide the composite system into two parts. While it can also be extended to multipartite states, the form of the decomposition differs in such cases.

However, not all states are pure states. In the case of mixed states, we have a separate definition of entanglement. A bipartite state, denoted as "row AB," is called separable if it can be expressed as a sum of terms, each representing a product state on the respective subsystems. The coefficients of these terms form a probability distribution. If a state cannot be expressed in this form, it is considered entangled.

Returning to our example of "Phi plus," we have determined that it is an entangled state. But can we describe the situation where Alice has access only to her qubit and has no knowledge of Bob's qubit, despite their entanglement? The answer lies in the concept of the partial trace.

The partial trace allows us to trace out one of the subsystems in a bipartite density operator. In the case of a bipartite density operator "row AB" and a basis for the Hilbert space of subsystem B, the partial trace over subsystem B is defined as the sum over the basis states of subsystem B, where we apply the identity operator on subsystem A and tensor it with the basis state of subsystem B. This operation is performed on both sides of

the density operator, and we sum over all the basis states of subsystem B.

By utilizing the partial trace, we can calculate the local density operator of the state "Phi plus." Taking the partial trace over Bob's qubit, we find that there are only two non-zero terms. One term corresponds to the state where Bob's qubit is in the zero state, and the other term corresponds to the state where Bob's qubit is in the one state. All other combinations give zero because they involve a combination of the zero and one states, resulting in a scalar product of zero.

Calculating the partial trace yields the sum of the zero state and the one state of Alice's qubit divided by two. This is known as the maximally mixed state, denoted as "PI A."

Understanding the Schmidt decomposition and the concept of the partial trace is essential in studying the fundamentals of quantum information carriers in the field of cybersecurity and quantum cryptography. These concepts allow us to analyze and determine the entanglement of states, as well as describe scenarios where subsystems are inaccessible to certain parties.

In the field of quantum cryptography, it is important to understand the fundamentals of quantum information carriers and composite quantum systems. One concept to grasp is the maximally mixed state, where both basis states of a system appear with equal probability. This state does not provide any useful information, as all possible basis states are equally probable.

When considering composite systems, such as those involving Alice and Bob, the local density operators for each individual system describe the situation in their respective labs. However, when one half of the system is lost or traced out, the information is lost as well. This means that the entangled state cannot be described solely by looking at the local density operators.

Another class of composite systems involves a classical system, denoted by the subscript "c". In this case, the states are tensor products of density matrices with classical values encoded into quantum states. These classical values are from a subset denoted by a calligraphic set. The corresponding ensemble is an ensemble of ensembles, where the state "rho a" comes from the ensemble itself. The density operator for this composite system is a sum over all possible classical values, weighted by the probability distribution "P set", multiplied by the tensor product states.

When discussing the evolution of composite systems, we consider quantum channels. A quantum channel is a linear, completely positive, and trace-preserving map. It can map between tensor products of Hilbert spaces. One special case is when the evolution only takes place on one subsystem, while the other subsystem remains invariant. This is known as the partial trace or discarding channel. The partial trace is a quantum channel on the B system, while the evolution on the A system is just the identity. The cross operators for the partial trace are the tensor product of the identity and the basis state on the Bob system.

Lastly, we explore the concept of the no-cloning theorem. This theorem states that it is impossible to perfectly copy unknown quantum states. If such a machine existed, it would allow for the copying of states without detection. However, the linearity of quantum mechanics prohibits the construction of such a machine. This is fortunate for quantum key distribution, as it ensures the security of the system.

Understanding the fundamentals of quantum information carriers and composite quantum systems is crucial in the field of cybersecurity. The maximally mixed state, local density operators, composite systems involving classical values, quantum channels, and the no-cloning theorem all play significant roles in quantum cryptography.

In the field of quantum cryptography, understanding the fundamentals of quantum information carriers is crucial. One important concept to grasp is the idea of composite quantum systems. In this context, we will explore the concept of a universal copier and the implications of the no-cloning theorem.

Let's consider a scenario where we have a state denoted as 'sy'. To duplicate this state, we can apply a copier, resulting in two copies of 'sy'. Mathematically, this can be represented as a linear combination of the basis states '0' and '1'. Specifically, we obtain the formula: '0 0', '0 1', '1 0', and '1 1', each with different amplitudes.

However, there is another way to calculate the action of this copier. By applying a unitary transformation 'U' to

the state 'sy' and considering the linear combination given by 'website', we can obtain a completely different result. In this case, the expression becomes 'alpha times 0 0' plus 'beta times 1 1'. It is important to note that these two expressions are generally not equal.

The no-cloning theorem states that a universal copier cannot exist for quantum states, except for a few specific cases. For classical states, it is possible to perfectly copy them. However, for quantum states, these two expressions are not equal, except when 'alpha' is equal to 1 and 'beta' is equal to 0, or when 'alpha' is equal to 0 and 'beta' is equal to 1.

Understanding the no-cloning theorem is crucial in the context of quantum key distribution, as it has implications for the security of the process. Additionally, we have briefly touched upon composite systems and how entanglement arises within them. Entropy will be discussed in the next material, as it plays a significant role in the security of quantum key distribution.

EITC/IS/QCF QUANTUM CRYPTOGRAPHY FUNDAMENTALS DIDACTIC MATERIALS
LESSON: ENTROPY
TOPIC: CLASSICAL ENTROPY

Classical entropy is an important concept in information theory that provides a mathematical framework for understanding the amount of information in a given system. It was first introduced by Claude Shannon in 1948 in his paper "A Mathematical Theory of Communication". In this paper, Shannon posed two fundamental questions about information: how much information can be compressed and stored, and how much information can be reliably transmitted through a communication channel.

To answer these questions, Shannon developed the concept of a random variable, which represents the possible outcomes of a random experiment. Each random variable has an alphabet, denoted as curly X, which consists of the possible realizations of the variable. For example, a coin flip can be represented by a random variable with the alphabet {heads, tails}.

The information content of a particular realization of a random variable is given by the negative logarithm of the probability of that realization occurring. This means that the more probable an event is, the less information it carries. Conversely, less probable events carry more information. The logarithm is taken to base two, which ensures that the unit of information is measured in bits.

The information content function has several important properties. Firstly, it only depends on the probability of the event, not on how the event is labeled. This means that the information content of a realization is the same regardless of how it is represented. For example, the information content of the realization 0 is the same as the information content of the realization plus, as long as they have the same probability of occurring.

Another property of the information content function is that it is monotonically decreasing with increasing probability. This means that as the probability of an event increases, the information content of that event decreases. This makes intuitive sense, as more probable events provide less surprising or unexpected information.

The concept of classical entropy builds upon the information content of individual realizations and extends it to the entire random variable. Classical entropy, denoted as H(X), is defined as the average information content of all possible realizations of the random variable X. It provides a measure of the uncertainty or randomness of the variable. The formula for classical entropy is given by:

$H(X) = -\Sigma P(x)\log_2(P(x))$

Where P(x) is the probability of the realization x occurring.

Classical entropy has several important properties. Firstly, it is always non-negative, meaning it is greater than or equal to zero. It is equal to zero when the random variable has only one possible realization with probability one, indicating complete certainty. On the other hand, it is maximized when all possible realizations are equally likely, indicating maximum uncertainty or randomness.

Classical entropy provides a fundamental measure of information in classical systems and serves as a basis for understanding and quantifying information in quantum systems. By learning about classical entropy and classical information theory, we can gain valuable insights and intuition that can help us understand and analyze quantum entropy and the choices of definitions made in quantum information theory.

Entropy is a fundamental concept in the field of cybersecurity, particularly in the realm of quantum cryptography. It is a measure of the uncertainty or randomness in a given system. In classical information theory, entropy is defined as the amount of information contained in a random variable.

There are several properties of entropy that are important to understand. Firstly, entropy is always non-negative and reaches its maximum value when all outcomes are equally likely. This means that a system with high entropy has more uncertainty and randomness. Conversely, a system with low entropy has less uncertainty and more predictability.

Secondly, entropy is continuous in the parameter of probability. If the probability of an event only slightly differs from another event, the information content of these events will also slightly differ. This property aligns with our intuition that similar events should have similar information content.

Thirdly, the information content of an event is high for unlikely events and low for more common events. This can be observed from a graph where as the probability of an event approaches one, the information content decreases. The information content can be thought of as the amount of surprise we experience when learning about a realization. If an event is very common, we are not surprised to see it occur, therefore the information content is low. Conversely, if the probability of an event is very low, we would be highly surprised to see it occur, leading to a high information content.

Lastly, the information content is additive. When two realizations of a random variable are assumed to be independent of each other, the information content of learning about a pair of realizations is the same as learning about the events individually. This is reflected in the calculation of the information content, where the sum of the individual information contents is obtained.

Moving beyond the information content of a single realization, we can define the entropy of a random variable. The entropy, often referred to as Shannon entropy after its creator Claude Shannon, is the measure of uncertainty or randomness in a discrete random variable. It is defined as the negative sum of the logarithm of the probabilities of individual realizations multiplied by their respective probabilities. This sum is taken over all possible realizations within the alphabet of the random variable.

It is important to note that when the probability of an event is zero, the logarithm of zero goes to negative infinity. To address this, a convention is used where zero times the logarithm of zero is considered to be zero. This is justified by the fact that an event with zero probability will never occur and should not contribute to the entropy of the random variable.

With the concept of entropy established, we can now address a question raised by Shannon in his 1948 paper. The question was how many bits are required to reliably compress a given amount of information. The answer to this question lies in Shannon's noiseless coding theorem, which states that the number of bits required for compression is equal to the entropy of the random variable that models the random experiment.

To better understand this concept, let's consider an example. Suppose we have a random variable with four possible outcomes: a, b, c, and d. The probabilities of these outcomes are as follows: a (1/2), b (1/4), c (1/8), and d (1/8). A simple compression scheme could be using 2 bits to encode each outcome. For example, we could encode a as 00, b as 01, c as 10, and d as 11. In this scheme, the expected length of a code word is 2.

However, according to Shannon, there exists a compressing scheme where the expected length of the code word is equal to the entropy of the random variable. To calculate the entropy, we can use the formula for entropy and substitute the probabilities of each outcome. In this case, the entropy of the random variable is calculated to be 7/4, which is less than the expected length of the code word in the simple compression scheme.

This example illustrates the concept that the entropy represents the minimum average number of bits required to encode each outcome of a random variable. By using a compression scheme that utilizes the entropy, we can achieve efficient and reliable compression of information.

Entropy is a fundamental concept in cybersecurity and quantum cryptography. It measures the uncertainty and randomness in a given system and plays a crucial role in information theory. Understanding the properties and calculations of entropy allows us to analyze and optimize compression schemes for reliable information storage and transmission.

In the field of cybersecurity, one of the fundamental concepts is entropy, which plays a crucial role in ensuring the security of cryptographic systems. Entropy measures the uncertainty or randomness of a random variable, and it is closely related to the amount of information contained in the variable. In this didactic material, we will explore the concept of entropy, particularly in the context of classical entropy.

One approach to encoding information is through the use of code words. In a scheme called variable length coding, code words are assigned to outcomes based on their probabilities. Outcomes with higher probabilities

are assigned shorter code words, while outcomes with lower probabilities are assigned longer code words. This approach allows for efficient encoding of information, as it minimizes the expected length of the code words.

For example, let's consider a variable with outcomes A, B, C, and D. We can encode A with the code word 0, B with 1 0, C with 1 1 0, and D with 1 1 1 0. By calculating the expected length of these code words, we find that it is equal to 7/4, which is the entropy of the random variable. This implies that we cannot achieve a lower expected length if we want to reliably decode the messages.

It is worth noting that we could use shorter code words for certain outcomes, such as encoding B with a single bit, but this would compromise the reliability of message decoding. Therefore, the chosen variable length coding scheme represents the best possible solution, aligning with Shannon's theorem.

Let's now shift our focus to binary entropy, which is a special case of entropy when there are only two outcomes. We denote these outcomes as 0 and 1, distributed according to a probability distribution where 0 occurs with probability P and 1 occurs with probability 1 - P. The binary entropy, denoted as H(P), can be calculated using the formula -P log P - (1 - P) log (1 - P).

The binary entropy is an essential concept that finds applications in various scenarios. When plotted as a function of the parameter P, it reaches its maximum value when P is equal to 1/2. This implies that when the probability is evenly distributed between the outcomes, we are most surprised by the events. In contrast, if the probability is biased towards one outcome, we would be less surprised and gain less information from observing that event.

Having explored examples of entropy and how it is computed, let's delve into some mathematical properties of the entropy function. Firstly, entropy is non-negative, as it represents the sum of positive information content weighted by the probabilities of the realizations. This property ensures that the entropy function yields a positive value.

Secondly, entropy is invariant to permutations of the realizations of the random variable. This property stems from the fact that entropy only depends on the probabilities of the realizations and not on the specific values of the realizations themselves.

Another property of entropy is that it vanishes if and only if the random variable is deterministic. A deterministic variable implies that there is only one value with a probability of 1, and all other values have a probability of 0. In this case, the entropy is equal to 0, as there is no uncertainty or randomness in the variable.

Lastly, the maximum value of entropy is given by the logarithm of the cardinality of the alphabet. For example, if we have four outcomes, the maximum entropy is the logarithm of four. Equality holds in this formula when the random variable is a uniform random variable.

Understanding the concept of entropy and its properties is crucial in the field of cybersecurity, as it provides insights into the security and reliability of cryptographic systems. By quantifying uncertainty and information content, entropy enables the design and evaluation of robust cryptographic algorithms.

Entropy is a fundamental concept in the field of cybersecurity, particularly in the context of quantum cryptography. In this didactic material, we will explore the concept of entropy and its variations, such as conditional entropy and joint entropy.

Entropy can be understood as a measure of uncertainty or randomness associated with a random variable. It quantifies the amount of information needed to describe the outcomes of a random experiment. The entropy of a random variable X is denoted as H(X) and is calculated using the formula:

$$H(X) = -\Sigma P(x) \log_2 P(x)$$

where P(x) represents the probability of a particular outcome x.

Conditional entropy, denoted as H(X|Y), is a measure of uncertainty in a random variable X given some side information Y. Consider a scenario where Alice and Bob are two parties involved in a random experiment. Alice holds the experiment and Bob has no knowledge about it initially. The uncertainty of Bob about the random

variable X is given by H(X). However, if Alice starts sending information to Bob, his uncertainty about X changes. It becomes the entropy of X conditioned on the side information Y, denoted as H(X|Y). Mathematically, it is defined as:

$$H(X|Y) = \Sigma P(x,y) \log_2 (P(x|y))$$

where P(x,y) is the joint probability distribution of X and Y, and P(x|y) is the conditional probability of X given Y.

The joint probability distribution, P(x,y), describes the probability of the occurrence of a pair (x,y) for two random variables X and Y. It can be expressed as the conditional probability distribution of X conditioned on Y, multiplied by the probability distribution of X. Using this joint probability distribution, we can define the joint entropy, denoted as H(X,Y), which is calculated as:

$$H(X,Y) = -\Sigma P(x,y) \log_2 P(x,y)$$

By substituting the joint probability distribution formula into the joint entropy formula, we can split the logarithm into two sums. This leads to the following equation:

$$H(X,Y) = H(X) + H(Y|X)$$

Alternatively, we can use a symmetric version of the formulas, replacing X and Y, to obtain:

$$H(X,Y) = H(Y) + H(X|Y)$$

It is important to note that conditioning does not increase the entropy of a random variable. Therefore, the entropy of a random variable X is always greater than or equal to the entropy of X conditioned on some side information, H(X|Y).

Entropy is a measure of uncertainty or randomness associated with a random variable. Conditional entropy quantifies uncertainty in a random variable given some side information. Joint entropy captures the combined uncertainty of two random variables. Understanding these concepts is crucial for analyzing and designing secure cryptographic systems.

The mutual information is a fundamental concept in classical information theory. It quantifies the amount of information that two random variables share. Given two random variables X and Y with a joint probability distribution P, the mutual information is defined as the entropy of X minus the conditional entropy of X given Y.

The entropy of X represents the uncertainty we have about the random variable X, while the conditional entropy of X given Y represents the uncertainty that remains about X after learning about Y. The difference between these two quantities is exactly the mutual information of X and Y, as it captures everything that can be learned about X from Y.

Similarly, the mutual information can also be defined as the entropy of Y minus the conditional entropy of Y given X. It is important to note that the mutual information is always non-negative. This can be easily seen from the formula, as the entropy of X is greater than or equal to the conditional entropy of X given Y.

To visualize the concept of mutual information, we can consider a diagram. The green circle represents the entropy of X, which is the uncertainty or information contained in X before learning about Y. The blue circle represents the entropy of Y, which is the information contained in Y. The overlap between the two circles represents the mutual information of X and Y, which can be learned from either X or Y.

In the case where X and Y are statistically independent, meaning there is no relationship between them, the circles are disjoint sets. In this case, the mutual information is outside of every circle and is equal to zero. This indicates that no information about X can be obtained from learning the outcomes of Y.

On the other hand, when X and Y are statistically dependent, the circles overlap, indicating that information about X can be obtained from learning about Y. The joint entropy of X and Y is the area covered by both circles. It is worth noting that the entropy of X conditioned on Y is equal to the entropy of X, and the same holds for the conditional entropy of Y given X. In this case, the joint entropy is the union of the two circles.

Now, let's address the question of how much information can be reliably transmitted through a given communication channel. Consider the scenario where Alice communicates with Bob over a classical channel. Alice holds a random variable X, and Bob receives information represented by a random variable Y. The capacity of the channel is defined as the maximum mutual information between X and Y, optimized over all possible probability distributions of X. This capacity represents the largest number of bits that Alice can reliably transmit over the channel.

We have explored the concept of mutual information in classical information theory. It quantifies the amount of shared information between two random variables. The mutual information is always non-negative and can be visualized using a diagram. Additionally, we have discussed the capacity of a communication channel, which represents the maximum amount of information that can be reliably transmitted. Classical information theory provides valuable insights into the transmission and processing of information.

Entropy is a fundamental concept in the field of cybersecurity, particularly in the context of quantum cryptography. In this didactic material, we will focus on classical entropy and its relevance to quantum entropy.

Classical entropy is a measure of uncertainty or randomness in a system. It quantifies the amount of information needed to describe the state of a system. The more uncertain or random the system, the higher its entropy.

In the context of cybersecurity, entropy plays a crucial role in generating secure cryptographic keys. Cryptographic keys are used to encrypt and decrypt sensitive information, and their security relies on the randomness of their generation. If a key can be easily guessed or predicted, it compromises the security of the system.

Entropy is commonly measured in bits. A bit is the basic unit of information and represents a binary choice between two options, typically represented as 0 or 1. The entropy of a system is directly related to the number of bits required to represent its state.

To generate secure cryptographic keys, it is essential to have a good source of entropy. This can be achieved by collecting data from unpredictable sources, such as atmospheric noise or hardware-based random number generators. The collected data is then processed to extract the randomness and convert it into a form suitable for generating cryptographic keys.

In the next material, we will delve into the concept of quantum entropy, which extends the principles of classical entropy to the realm of quantum mechanics. Quantum entropy introduces new challenges and opportunities for secure communication and cryptography. So let us then continue for an in-depth exploration of quantum entropy and its applications in the field of cybersecurity.

EITC/IS/QCF QUANTUM CRYPTOGRAPHY FUNDAMENTALS DIDACTIC MATERIALS
LESSON: ENTROPY
TOPIC: QUANTUM ENTROPY

In the study of quantum key distribution, it is important to understand the concept of quantum entropy. Quantum entropy is a measure of uncertainty in a quantum system, similar to how classical entropy quantifies uncertainty in a classical system. Although the definitions and formulas for quantum entropy resemble their classical counterparts, there are some properties unique to the quantum world.

To define the quantum entropy of a state, let's consider a quantum system A in state ρ. The entropy of the state, denoted as S(ρ), is given by the formula $S(\rho) = -Tr(\rho \log \rho)$, where Tr denotes the trace operation. This definition is similar to the classical definition of entropy, with the logarithm of the state ρ replacing the probability distribution.

If we know the spectral decomposition of the state ρ, where $\rho = \Sigma\lambda_i|\psi_i\rangle\langle\psi_i|$ and λ_i are the eigenvalues, then the entropy can be expressed as $S(\rho) = -\Sigma\lambda_i \log \lambda_i$. This resembles the Shannon entropy of a random variable modeled by the eigenvalues of ρ. Just like in the classical case, the eigenvalues form a probability distribution, summing up to one.

The interpretation of quantum entropy becomes clear when we consider two parties, Alice and Bob. Alice prepares quantum states $|\psi_x\rangle$ with a probability $P(_x)$, and Bob wants to determine Alice's state from his perspective. Bob's uncertainty about Alice's state can be quantified by calculating the quantum entropy of the state ρ, which is formed by the ensemble of states $|\psi_x\rangle$ and their corresponding probabilities $P(_x)$. This is analogous to the classical case, where uncertainty is quantified by the entropy of the random variable modeling the experiment.

Now, let's discuss some mathematical properties of quantum entropy. Firstly, the quantum entropy of a state is always non-negative for all identity operators. This follows from the fact that the quantum entropy is a function of the eigenvalues, just like the classical entropy.

Secondly, the quantum entropy of a state is zero if and only if the state is a pure state. To prove this, suppose the quantum entropy vanishes. This implies that all eigenvalues λ_i must be either 0 or 1. If λ_i equals 1 for a certain index J, then all other eigenvalues must be 0, indicating a pure state. On the other hand, if the state is pure, meaning it has only one non-zero eigenvalue, the entropy is directly calculated as -log(1), which equals 0.

Lastly, the value of quantum entropy is upper bounded by the logarithm of the dimension of the system. This means that the entropy cannot exceed a certain value determined by the system's dimension.

Quantum entropy is a measure of uncertainty in a quantum system, similar to classical entropy. It quantifies the uncertainty about a quantum state and plays a crucial role in understanding quantum key distribution. Understanding the properties of quantum entropy helps us analyze and interpret quantum systems effectively.

In the field of quantum cryptography, understanding the concept of entropy is crucial. Entropy measures the uncertainty or randomness in a system. In classical cryptography, the entropy was bounded by the logarithm of the alphabet size. Similarly, in quantum cryptography, the entropy can be proven to have similar properties. One important property to note is that applying an isometry to a quantum state does not change its entropy. This means that when we apply a matrix B to a state from both the right and the left, the entropy remains unchanged. The only effect of this operation is to transfer one orthonormal basis to another. Since entropy is only dependent on the eigenvalues of the state, and the eigenvalues remain unchanged, the entropy remains the same.

After understanding the definition and properties of quantum entropy, it is important to explore different variants of entropy. Many of these variants are analogous to classical entropy, such as joint entropy, conditional entropy, and mutual information. However, one variant called coherent information is unique to quantum cryptography.

Let's start with the joint quantum entropy. If we have a bipartite quantum state, denoted as Rho_AB, the joint entropy of the state is defined as the negative trace of the bipartite state multiplied by the logarithm of the

bipartite state. This definition is analogous to the definition of quantum entropy for a single system, but now we consider a bipartite state instead. In classical joint entropy, it is always greater than or equal to the entropy of either random variable individually. However, in the quantum world, these inequalities are not always fulfilled. An example of this is a pure bipartite state, where the joint entropy is zero. This is because the entropy of a single system is zero for a pure state, and the joint entropy follows the same reasoning.

Now, let's consider the marginal entropy. The marginal states for system A and system B are obtained from the Schmidt decomposition of the pure bipartite state. The eigenvalues of the marginal states are the same in both cases. Interestingly, while the joint entropy is zero for a pure bipartite state, the marginal entropies do not necessarily have to be zero. They can be zero in some special cases, but in general, they can have non-zero values. However, what is even more intriguing is that the entropies of the marginal states are always the same. This is a significant difference from the classical case, where the entropies of the marginal states can be different. An example of this can be seen with the bipartite entangled state Phi+ (0 0 + 1 1 divided by the square root of 2). The marginal states for both systems are maximally mixed states, and their entropies are logarithm base 2 of 2, which equals 1. This example demonstrates that the inequality that holds in classical cases is not fulfilled in the quantum world.

Moving on to conditional quantum entropy, the definition is analogous to classical conditional entropy. If we have a bipartite quantum state Rho_AB, the conditional entropy of system A conditioned on system B is defined as the joint entropy of system A and system B minus the entropy of system B. This definition holds for both joint quantum entropy and conditional quantum entropy.

Understanding entropy in the context of quantum cryptography is crucial. The concept of entropy measures the uncertainty or randomness in a system. In quantum cryptography, the properties of entropy are similar to classical cryptography, but there are also unique characteristics. Joint quantum entropy, marginal entropy, and conditional quantum entropy are important variants to consider. It is important to note that the inequalities that hold in classical cases are not always fulfilled in the quantum world.

The concept of quantum entropy plays a fundamental role in the field of cybersecurity, specifically in quantum cryptography. In this context, entropy refers to the measure of uncertainty or randomness in a system. Quantum entropy is a concept that arises from the principles of quantum mechanics, which govern the behavior of particles at the quantum level.

In the context of quantum cryptography, one important aspect to consider is conditional quantum entropy. This refers to the amount of uncertainty or randomness in a joint quantum system, given the knowledge of its individual parts. To calculate conditional quantum entropy, we subtract the marginal entropy (entropy of the individual parts) from the joint entropy (entropy of the joint system).

In a specific example, let's consider the state of a quantum system. If we calculate the joint entropy and the marginal entropy, we can then determine the conditional entropy. It is important to note that in the quantum case, the conditional entropy can be negative, which is not possible in classical systems. This negative value indicates that we have more knowledge about the joint system than its individual parts. This phenomenon occurs when the system is in an entangled state, where the joint system is well-defined, but the individual parts are described by maximally mixed states.

This distinction between quantum and classical systems is significant, as it highlights a unique characteristic of the quantum world. In fact, a theorem can be proven, stating that for all pure bipartite entangled states, the conditional entropy is zero. Conversely, whenever we encounter negative conditional entropy for a pure bipartite state, we can conclude that it is entangled.

To further explore the concept of conditional quantum entropy, researchers have defined a quantity known as the quantum coherent information. This quantity is the negative of the conditional quantum entropy and is useful in various applications within quantum cryptography. It is worth noting that the quantum coherent information does not exist in classical systems, as it is not meaningful to consider the negative of the conditional information in that context.

Another relevant concept is the quantum mutual information, which is analogous to the classical mutual information. It is calculated by adding the entropies of the individual systems and subtracting the joint entropy. The quantum mutual information provides insights into the correlation between the two systems.

The study of quantum entropy, particularly conditional quantum entropy, is essential in the field of cybersecurity, specifically in quantum cryptography. It allows us to understand the level of uncertainty and randomness in joint quantum systems, as well as the relationship between the individual parts and the joint system. The distinction between quantum and classical systems in terms of entropy highlights the unique characteristics of the quantum world.

In the field of quantum cryptography, the concept of entropy plays a crucial role. Entropy is a measure of uncertainty or randomness in a system. In classical information theory, entropy is well-defined and has operational interpretations. However, when it comes to quantum information theory, the notion of uncertainty based on Heisenberg's uncertainty principle is unsatisfactory.

Heisenberg's uncertainty principle, which relates the uncertainty between the measurement of position and momentum, does not have a nice operational interpretation in information theoretic tasks. Additionally, it does not take into account the fact that quantum systems can be entangled or correlated.

To address these issues, we need an uncertainty principle that is formulated in terms of entropy. Entropy provides a more suitable measure of uncertainty in quantum scenarios and can account for system correlations. By formulating an uncertainty principle in terms of entropy, we can better understand and analyze quantum cryptographic tasks.

Let's consider an example to illustrate the limitations of Heisenberg's uncertainty relation. Suppose we have an entangled state, denoted as Phi plus, which can be expressed in the computational basis or the Mohammed basis. If Alice measures her part of the system using the Z operator, she can predict her outcome with certainty. By communicating her measurement to Bob, he can also determine Alice's outcome by measuring his part of the system in the respective bases. Similarly, if Alice measures using the X operator, Bob can predict her outcome with certainty once he knows the measurement basis.

This seems to contradict Heisenberg's uncertainty relation, which states that Z and X measurements are incompatible. The problem lies in the fact that Heisenberg's uncertainty principle does not consider the entanglement between the two systems. To overcome this limitation, we need an uncertainty principle that takes into account the entanglement and is formulated in terms of entropy.

To define such an uncertainty principle, let's consider a scenario where Bob prepares a bipartite quantum state and sends one part to Alice. Alice can then choose between two measurements, Z or X. After her measurement, she communicates her choice to Bob. The uncertainty that Bob has about Alice's outcome can be quantified using entropy.

In a more general setting, Alice can choose between multiple measurements described by POVMs (Positive Operator Valued Measures). Suppose she chooses to measure the POV M described by M. The state after her measurement, denoted as Sigma XP, can be expressed as a product of the outcome X encoded into quantum states and the trace of Alice's system with the state row ad, which represents Bob's part of the system.

By analyzing the state that Bob holds after Alice's measurement and the measurement outcome, we can quantify the uncertainty that Bob has about Alice's outcome using entropy. This uncertainty principle, formulated in terms of entropy, provides a more comprehensive understanding of the uncertainty in quantum cryptographic tasks.

The concept of entropy is crucial in quantum cryptography. By formulating an uncertainty principle in terms of entropy, we can overcome the limitations of Heisenberg's uncertainty relation and better analyze information theoretic tasks in the quantum realm.

In the field of cybersecurity, one important concept to understand is quantum cryptography, specifically the fundamentals of entropy and quantum entropy. Entropy refers to the uncertainty or randomness associated with a system or variable. In the context of quantum cryptography, entropy plays a crucial role in quantifying the uncertainty or unpredictability of certain measurements.

To begin, let's consider a scenario where Alice and Bob are communicating using quantum systems. Alice performs a measurement using a POV (Positive Operator Valued) element denoted as M, and Bob's uncertainty

about Alice's outcome is described by the conditional quantum entropy of X. This entropy is conditioned on Bob's quantum system.

Now, if Alice measures a different POV element, denoted as N, the state remains similar, but the outcomes are different. Bob's uncertainty, in this case, can be quantified by the conditional entropy of a random variable, conditioned on Bob's system, and evaluated over the state.

To determine Bob's total uncertainty, we need to consider the uncertainty about both measurements. This can be done by simply summing the two conditional entropies.

Similar to the Heisenberg uncertainty principle, we aim to establish a lower bound on the uncertainty. In this case, the lower bound is given by the logarithm of one plus the conditional entropy of A conditioned on B and C. Here, C represents the incompatibility of the two POV elements that Alice can measure.

The incompatibility, denoted by C, is a quantity that depends only on the two POV elements and not on the system's state. It is given by the maximum over all possible POV elements, where the index "accent" represents the infinity norm of the operator. In the finite-dimensional case, the infinity norm corresponds to the largest eigenvalue of the operator.

This entropic uncertainty principle provides a framework for the scenario described. It consists of two terms: one that depends on the incompatibility of the measurements and another that depends on the system's state. It is worth noting that, since the conditional entropy can be negative, the lower bound of uncertainty can be lower than the term representing incompatibility. This means that, by choosing the right state for measurement, the uncertainty can be reduced to zero in some cases.

Although we won't prove this lower bound here, it has been established in a paper by Mario Berta and others, published in Nature Physics, titled "The Uncertainty Principle in the Presence of Quantum Memory."

Now, let's consider an example using the familiar quantum state $|+\rangle$ and the POV elements for the X measurement. The probability distribution function (PDF) for this measurement is constructed using the POV elements and the zero state and the one state. By calculating the parameter C, we find it to be equal to one-half. Additionally, we have previously calculated the conditional entropy of this state to be -1.

By evaluating the entropic uncertainty lower bound, we obtain the logarithm of 2, which is 1, minus the conditional entropy (-1), plus the conditional entropy (-1), resulting in 0. This is consistent with our observation that, in the described scenario, Bob can predict the outcome with certainty.

In contrast to Heisenberg's uncertainty principle, the entropic uncertainty principle accurately represents the possibility of achieving zero uncertainty in certain cases. This makes it a valuable tool for information-theoretical tasks in quantum cryptography.

To summarize, in this material, we have covered the concept of quantum entropy, different variants of quantum entropy, and some surprising observations. We have also explored the entropic uncertainty principle and its implications. With this understanding, we have equipped ourselves with the necessary mathematical tools and knowledge of entropy. In the next material, we will delve into quantum key distribution (QKD) protocols, discussing their preparation, differences from entanglement-based protocols, and the step-by-step process involved.

EITC/IS/QCF QUANTUM CRYPTOGRAPHY FUNDAMENTALS DIDACTIC MATERIALS
LESSON: QUANTUM KEY DISTRIBUTION
TOPIC: PREPARE AND MEASURE PROTOCOLS

Quantum key distribution is a fundamental concept in cybersecurity that aims to establish a secret key between two distant parties, typically referred to as Alice and Bob. This secret key can be used to encrypt and decrypt messages, ensuring secure communication. In this didactic material, we will focus on the quantum transmission phase of quantum key distribution protocols, particularly the prepare and measure schemes.

The quantum transmission phase is the first part of a quantum key distribution protocol, where the actual quantum operations take place. During this phase, Alice and Bob exchange or measure quantum states, or an independent source distributes quantum states to them. At the end of this phase, both Alice and Bob hold a bit string, which is partially correlated and partially secure.

The second part of a quantum key distribution protocol is the classical post-processing phase. In this phase, Alice and Bob take the bit strings obtained from the quantum transmission phase and perform error correction and privacy amplification to enhance the security of the key. The goal is to transform the partially secure bit strings into a fully secure key that can be used for encryption schemes like the one-time pad.

There are two main types of quantum key distribution protocols: prepare and measure schemes, and entanglement-based schemes. In prepare and measure schemes, Alice prepares and sends quantum states to Bob, who measures them. On the other hand, entanglement-based schemes involve Alice and Bob holding entangled pairs of qubits, which can be prepared by either Alice, Bob, or a third party. In this didactic material, we will focus on prepare and measure protocols.

The general structure of a prepare and measure protocol involves Alice and Bob having a quantum channel and a classical channel. The quantum channel allows Alice to send quantum states to Bob, while the classical channel enables them to exchange messages. The classical channel is authenticated, ensuring that Alice and Bob can verify each other's identities. It is important to note that Eve, a potential eavesdropper, can listen to the quantum and classical communication but cannot alter the classical communication.

One well-known example of a prepare and measure protocol is the BB84 protocol, introduced in 1984 by Charles Bennett and Gilles Brassard. In the BB84 protocol, Alice chooses two random bit strings: string A and string B, each consisting of 4n bits. String A contains the actual key bits, while string B determines the basis in which the qubits will be measured.

The BB84 protocol proceeds as follows: Alice prepares a qubit in one of four possible states, representing the two bases and the two values of the bit. She then sends the qubits to Bob through the quantum channel. Bob randomly chooses a measurement basis for each qubit and performs the measurement. After the measurement, Alice and Bob publicly announce the bases they used for each qubit. They discard the qubits measured in different bases and keep the remaining qubits with matching bases. These matching qubits form their partially correlated and partially secure bit strings.

The quantum transmission phase of a quantum key distribution protocol involves the exchange or measurement of quantum states between Alice and Bob. The prepare and measure schemes are a type of protocol where Alice prepares and sends quantum states to Bob. The BB84 protocol is an example of a prepare and measure protocol, where Alice and Bob exchange qubits in different bases to establish a secret key. By understanding the fundamentals of quantum key distribution protocols, we can enhance the security of communication in the field of cybersecurity.

In the field of quantum cryptography, one of the fundamental concepts is Quantum Key Distribution (QKD). QKD is a method used to securely distribute cryptographic keys between two parties, commonly referred to as Alice and Bob, over a quantum channel. The goal is to establish a shared secret key that can be used for secure communication.

In the prepare and measure protocol of QKD, Alice prepares quantum states based on a key bit string and a basis string. The key bit string determines whether Alice uses the computational basis or the Hadamard basis to encode the bits. The basis string determines the basis for each qubit, resulting in four possible states.

Alice sends these prepared states to Bob over a quantum channel. In an ideal scenario, the quantum channel is free from noise and losses. Bob receives the states and announces his choice of basis. Alice then measures the states based on Bob's announcement. Both Alice and Bob hold two bit strings: one storing the actual key bits and the other storing the chosen bases for measurements.

In the sifting step, Alice and Bob compare their chosen bases. Alice announces her choice of basis, but only after Bob has received the qubits. Bob then announces the positions where his chosen basis differs from Alice's. These differing positions indicate a different basis choice and are discarded.

After the sifting step, Alice and Bob have bit strings of length 2N, where N is the length of the original key bit string. The probability of Bob choosing the wrong basis is 50%, resulting in a 50% difference between their bit strings.

The next phase is classical post-processing, where Alice and Bob use classical messages to estimate the information gained by a potential eavesdropper, perform error correction to make their bit strings identical, and perform privacy amplification to ensure the key remains secret.

An interception-resend strategy is a simple strategy that an eavesdropper, commonly referred to as Eve, can perform. Eve intercepts all the qubits sent by Alice to Bob. Since Eve doesn't know the basis chosen by Alice, she randomly guesses the basis and measures the qubits. In half of the cases, Eve guesses correctly, resulting in perfectly correlated bits with Alice. In the other half of the cases, Eve's guess is wrong, resulting in completely random results.

In the field of cybersecurity, quantum cryptography is a cutting-edge technology that aims to provide secure communication channels by leveraging the principles of quantum mechanics. One of the fundamental concepts in quantum cryptography is Quantum Key Distribution (QKD), which allows two parties, Alice and Bob, to establish a shared secret key that can be used for secure communication.

In the QKD protocol, Alice prepares a series of quantum bits or qubits in a specific basis and sends them to Bob over a quantum channel. However, an eavesdropper, Eve, may try to intercept and gain knowledge about the qubits. To detect eavesdropping attempts, Alice and Bob employ a prepare and measure protocol.

In this protocol, Alice prepares each qubit in a specific basis and sends it to Bob. Bob then measures the qubits in a randomly chosen basis, without any knowledge about the basis chosen by Alice. In the sifting step, Alice and Bob compare the bases they used and obtain key bit strings. If they have chosen the same basis, they are sure that there is no error in their key bit strings. However, if they have chosen different bases, there is a possibility of error.

In half of the cases, Alice and Bob choose the same basis, resulting in no error. In the other half, they choose different bases, leading to a 25% error rate. If Alice and Bob observe a high error rate, they can infer that Eve has intercepted the qubits and gained knowledge about the key. In such cases, they would likely abort the protocol to ensure secure communication.

To illustrate this protocol, let's consider an example with Alice sending 10 qubits to Bob. Alice first chooses a key bit string, denoted as 'a', and a basis string, denoted as 'b'. The choice of 'b' determines the basis in which Alice encodes each key bit. For example, if 'b' is 'C' (computational basis), the corresponding qubit is '0'. If 'b' is 'H' (Hadamard basis), the corresponding qubit is '1'.

Alice then prepares the quantum states based on the chosen 'a' and 'b' strings. These preparations result in a list of quantum states. However, since we are considering eavesdropping, Eve intercepts the states and measures them in a randomly chosen basis. She then prepares the quantum states she measured and sends them to Bob.

Bob, unaware of the basis chosen by Alice or Eve, randomly chooses a basis to measure the received qubits. His measurements result in a set of measured states. In the sifting step, Alice and Bob compare the bases they used and obtain the final key bit strings.

By analyzing the example, we can observe that when Eve chooses the wrong basis, there is an error in the

received states. Conversely, when Eve chooses the right basis, the received states match the ones initially prepared by Alice. This comparison allows Alice and Bob to detect eavesdropping attempts.

The prepare and measure protocol in quantum key distribution enables Alice and Bob to establish a secure shared key by detecting and preventing eavesdropping attempts. By comparing the bases used in the protocol, they can identify errors and ensure the security of their communication.

In quantum key distribution, the goal is to securely distribute a shared key between two parties, Alice and Bob, in the presence of a potential eavesdropper, Eve. One popular approach is the prepare and measure protocol, which includes the BB84 protocol, the six state protocol, and the SARG04 protocol.

In the BB84 protocol, Alice prepares qubits in either the computational basis (Z) or the Hadamard basis (X) and sends them to Bob. Bob randomly chooses to measure each qubit in either the computational basis or the Hadamard basis. If Bob measures in the same basis as Alice prepared, the key bit is preserved. If Bob measures in a different basis, the key bit is discarded. By comparing a subset of their key bits, Alice and Bob can estimate the error rate introduced by Eve's potential eavesdropping.

The six state protocol is similar to the BB84 protocol, but introduces a third basis, the Y basis. Alice prepares qubits in either the Z, X, or Y basis and sends them to Bob. Bob randomly chooses to measure each qubit in one of the three bases. Again, by comparing a subset of their key bits, Alice and Bob can estimate the error rate introduced by Eve.

The SARG04 protocol is designed to be secure against a specific attack called the filter number splitting attack. In this attack, Eve intercepts the qubits during the transmission phase. The SARG04 protocol includes additional steps to prevent this attack.

The prepare and measure protocols, including BB84, six state, and SARG04, provide a means for secure key distribution in the presence of potential eavesdroppers. Each protocol has its own advantages and considerations, such as the number of bases used and the security against specific attacks.

In the field of quantum cryptography, one of the fundamental concepts is quantum key distribution (QKD). QKD is a method used to securely exchange cryptographic keys between two parties, typically referred to as Alice and Bob, over a potentially insecure communication channel. One of the commonly used protocols for QKD is the prepare and measure protocol.

To implement the prepare and measure protocol, a perfect single photon source is required. However, in reality, such ideal sources do not exist. Experimentalists often use weak laser pulses to encode the qubits. In these weak laser pulses, there is typically no photon present in about 90% of the cases. However, in the remaining 10% of the cases, there is a single photon present, which is the desired scenario. Occasionally, there may be more than one photon in a pulse, which poses a security threat.

If a laser pulse contains more than one photon, an attacker, referred to as Eve, can perform a specific attack. Eve can store one of the photons in a quantum memory and announce that she has received photons. When Alice announces the basis she used for encoding, Eve can measure her stored photon using the correct basis and obtain a perfectly correlated bit value. This allows Eve to gain perfect knowledge about the key, making it difficult for Alice and Bob to detect this attack.

To address this vulnerability, researchers have developed protocols, such as the SAR go4 protocol, that are secure against attacks involving multiple photons. These protocols modify the sifting step, which is the step where Alice and Bob compare their measurement results to determine the validity of the key bit.

In the SAR go4 protocol, the sifting step differs from previous protocols. Let's consider an example to understand how it works. Suppose Alice sends the state |00|. In this case, the first bit should not be considered as the key bit and the second bit as the basis bit. Instead, the key bit is determined by the basis Alice used for encoding. After Bob measures the received state, Alice announces a pair of states. One of the states in the pair is the state Alice actually sent, and the other state is from a different basis. In this example, the state Alice sent is in the computational basis, so the second state in the pair must be from the X basis. The secret key bit, in this case, is 0 because the 0 indicates that the state Alice prepared and sent was in the computational basis.

Bob then examines his measurement result and determines whether the bit is valid or invalid. If Bob can distinguish between the two candidate states based on his measurement result, he can conclude which state Alice sent and determine the secret key bit. However, there are scenarios where Bob cannot distinguish between the candidate states, leading to an invalid bit.

For instance, if Bob measures in the computational basis or the Z basis and obtains the result |00|, it is consistent with both the state |00| and the state |01|. Therefore, Bob cannot determine which state Alice sent, and he declares the bit as invalid. Another scenario is when Bob measures in the Hadamard basis, resulting in a random outcome of either |01| or |11|.

The prepare and measure protocol is a method used in quantum key distribution to securely exchange cryptographic keys. However, the presence of multiple photons in a laser pulse can lead to security vulnerabilities. Protocols like the SAR go4 protocol address this issue by modifying the sifting step. By carefully comparing measurement results, Alice and Bob can determine the validity of the key bits and establish a secure communication channel.

In this didactic material, we will discuss the fundamentals of quantum cryptography, specifically focusing on quantum key distribution using prepare and measure protocols. We will explore the steps involved in these protocols and understand the concept of eavesdropping.

Quantum key distribution (QKD) is a cryptographic technique that utilizes the principles of quantum mechanics to establish secure communication channels. Prepare and measure protocols are one type of QKD protocol, where the sender, Alice, prepares quantum states and the receiver, Bob, measures them to establish a shared secret key.

In the prepare and measure protocol, Alice prepares quantum states, typically using photons, in a specific basis. She then sends these states to Bob over a quantum channel. Bob receives the states and performs measurements in a randomly chosen basis. The choice of basis is kept secret until the end of the protocol.

To ensure the security of the key distribution, Alice and Bob perform a sifting procedure. They compare the basis used by Alice for encoding with the basis used by Bob for measurement. If the bases match, they keep the corresponding measurement outcome as a valid bit of the secret key. If the bases do not match, the bit is discarded.

In the case where the measurement outcomes indicate a basis mismatch, the bit is considered invalid. However, if the outcomes match, the bit is considered valid. By repeating this process for multiple quantum states, Alice and Bob can establish a shared secret key.

It is worth noting that the sifting procedure in prepare and measure protocols is more complex compared to other protocols, such as the BB84 protocol. In prepare and measure protocols, more bits may be discarded as invalid due to basis mismatches. Despite this drawback, prepare and measure protocols offer the advantage of not requiring Alice to announce the basis used for encoding, enhancing the security of the protocol.

Now, let's briefly discuss eavesdropping. In quantum cryptography, eavesdropping refers to an unauthorized third party, Eve, attempting to gain information about the secret key being established between Alice and Bob. One common attack is the photon number splitting attack, where Eve stores the photons sent by Alice and measures them later.

However, in the prepare and measure protocol, Eve does not have access to the basis used by Alice for encoding. Therefore, she cannot obtain the information required to measure the bit correctly. This makes the protocol secure against the photon number splitting attack.

It is important to note that while prepare and measure protocols are secure against specific attacks, other protocols may be more suitable for different types of attacks. Each protocol is tailored to address specific security concerns.

This didactic material has provided an overview of prepare and measure protocols in quantum key distribution. We have discussed the steps involved in these protocols, the sifting procedure, and the concept of eavesdropping. In the next part, we will explore entanglement-based protocols and their equivalence to prepare

and measure protocols.

EITC/IS/QCF QUANTUM CRYPTOGRAPHY FUNDAMENTALS DIDACTIC MATERIALS
LESSON: ENTANGLEMENT BASED QUANTUM KEY DISTRIBUTION
TOPIC: ENTANGLEMENT BASED PROTOCOLS

Welcome to this educational material on entanglement-based quantum key distribution protocols in the field of cybersecurity. In our previous discussion, we explored prepare and measure protocols. Now, we will delve into a different class of protocols known as entanglement-based protocols.

A quantum key distribution protocol consists of two main parts: the quantum transmission phase and the classical post-processing phase. So far, we have focused on the quantum transmission part. In this phase, we can employ either a prepare and measure protocol or an entanglement-based protocol. Today, we will focus on the latter.

The concept behind entanglement-based protocols involves two parties, Alice and Bob, who have access to a source denoted as 's' in the diagram. This source distributes quantum states, and it can be under the control of Alice, Bob, a third party called Charlie, or even Eve. We do not make any assumptions about the source, and we account for the worst-case scenario where Eve has total control over it.

Additionally, Alice and Bob have access to a classical channel through which they can exchange classical messages. This channel serves a similar purpose as in the prepare and measure protocol. However, in this case, we assume that Eve can listen to the communication over the classical channel without being able to change it.

Let's now explore an example of an entanglement-based protocol to understand its structure. The first protocol we will discuss is called the "get protocol," invented by Arthur in 1991. This protocol utilizes maximally entangled states to generate a key. If the source distributes maximally entangled states to Alice and Bob, and they can verify this, it becomes impossible for Eve to have any information about the state. This is due to the monogamy of entanglement, which states that if two parties share a maximally entangled state, a third party cannot have any entanglement with that state.

To implement the get protocol, Alice and Bob perform specific measurement operations. These measurements are best depicted on the Bloch sphere, where the x-axis represents the horizontal axis and the z-axis represents the vertical axis. Alice's measurement operations are depicted on the left side, while Bob's are on the right side.

Alice's measurements include a z-axis measurement (a1), an x-axis measurement (a2), and a linear combination of both (a3). Similarly, Bob's measurements consist of b1, b2, and b3, which correspond to the same measurement operations as Alice's.

By choosing specific pairs of measurements, such as a1 and b1 or a3 and b3, Alice and Bob can generate a key. These pairs ensure that they measure in the same basis, resulting in completely anti-correlated qubits, which they can use as a key.

However, Alice and Bob also need to assess the information Eve may have about the state. To do this, they utilize other measurement directions, namely a1-b3, a1-b2, a2-b3, and a2-b2. They employ the CHSH inequality to test how much information Eve possesses. This inequality is derived for classical random variables denoted as a1, a2, b3, and b2, which correspond to the measurement directions.

Entanglement-based protocols in quantum key distribution leverage maximally entangled states to generate secure keys. By performing specific measurement operations and utilizing the CHSH inequality, Alice and Bob can assess the information Eve may have on the state and ensure the security of their key.

In the field of quantum cryptography, entanglement-based quantum key distribution (QKD) protocols play a crucial role in ensuring secure communication. One such protocol is the Echod protocol, which is based on the violation of the Clauser-Horne-Shimony-Holt (CHSH) inequality.

To understand the Echod protocol, let's first discuss the classical case. In this case, we have classical random variables that can take the values of plus one or minus one with equal probability. By calculating the term a1*B3 + B2 + a2*b3 - b2, we find that the result is either plus two or minus two. Taking the expectation value of this term, we find that it is always less than or equal to two. This inequality is known as the CHSH inequality,

denoted by S. In the classical case, S is always less than or equal to two.

Now, let's move on to the quantum case. In the quantum case, we have quantum observables a1, a2, b3, and b2. The expectation value in the quantum case is defined as the trace over the tensor product of the measurement operators (a1⊗b3)⊗(a2⊗b2) times the state ρ. For example, in the Echod protocol, if we want to calculate the expectation value of a1 and b3, we can use the measurement operators a1 = (1/√2)(a + X) and b3 = (1/√2)(a + X), and calculate the expectation value with respect to the state ρ. The result of this calculation is -1/√2.

By calculating the expectation values for all the terms in the definition of the CHSH value, we find that the result is 2√2, which is greater than 2. This violates the classical CHSH inequality. If we have a maximally entangled state, the CHSH value is always 2√2. Therefore, by checking the CHSH value for these pairs of measurements, we can determine if there is entanglement present in the state. If the value is 2 or less, there is no entanglement, and it is not possible to generate a secure key. If the value is between 2 and 2√2, we can use classical post-processing techniques to turn the partially correlated and partially secret key into a secure key.

Now, let's summarize the Echod protocol step by step. First, Alice and Bob distribute a number of entangled states between them. It doesn't matter how they do this, whether one of them has the source and distributes the states or they get them from a third party. For each state, Alice and Bob randomly choose a measurement from their respective sets of measurements and announce the basis they chose. The measurement results for the pairs a1b1 and a3b3 form the sifted key. The sifted key is obtained by discarding the bits where they chose different basis states. The remaining results are used to test the CHSH inequality. If the results pass the test, indicating that the CHSH value is higher than 2, they proceed with error correction and privacy amplification to turn the partially secret and partially correlated bit strings into a secure key that can be used for cryptography applications.

Now, let's take a look at another entanglement-based protocol, the BB84 protocol. This protocol is a variation of the BB84 protocol, but instead of using single qubits, it uses pairs of maximally entangled states. The goal is still to distribute these entangled states between Alice and Bob for key generation.

Entanglement-based quantum key distribution protocols, such as the Echod protocol and the entanglement-based version of the BB84 protocol, provide a secure way of distributing keys for cryptographic applications. By leveraging the properties of entangled states and testing the violation of certain inequalities, these protocols ensure the generation of secure keys for communication.

In quantum cryptography, one of the fundamental concepts is entanglement-based quantum key distribution. This protocol involves the distribution of perfectly entangled states to generate a secure key. To achieve this, certain quantum error correction codes, known as Calderbank-Shor-Steane codes, are used.

The key generation process relies on the construction of the Calderbank-Shor-Steane code, which involves taking two classical error correction codes, denoted as C1 and C2, that can correct key errors. These codes are used to encode m qubits into n qubits, where n must be greater than m. The resulting quantum error correction code can correct up to T errors.

The entanglement-based protocol begins with Alice creating 2n cubed pairs, with each qubit in a Hadamard state. She randomly selects qubits from this set to estimate the errors in the qubit pairs. Alice also selects a random classical bit string, B, of length 2n, with one bit for each qubit pair. If the bit value at position I is 1, she applies a Hadamard transformation to her half of the corresponding qubit pair.

Alice then sends the other half of the qubit pairs to Bob, along with the string B and the positions of the check qubits. Bob applies a Hadamard transformation to the qubits for which the corresponding bit value is 1. This transformation prepares the qubits in a Hadamard basis. From Bob's side, measuring in the Hadamard basis is equivalent to measuring in the computational basis.

The next step involves Alice and Bob measuring the check qubits in the computational basis to estimate the error rate. If they observe more than T errors, the protocol is aborted, as the quantum error correction code can only correct up to T errors. If the number of errors is below T, Alice and Bob use the Calderbank-Shor-Steane code to correct the errors in the remaining bits. They obtain M copies of the Phi+ state, where M is the number of remaining bits.

With the knowledge that they have shared maximally entangled states, Alice and Bob can measure the Phi+ states in the computational basis to obtain a shared secret key. The protocol is designed to ensure that no party has any knowledge of the state after measurement, ensuring the security of the key.

It is important to note that this entanglement-based protocol is equivalent to the prepare-and-measure BB84 protocol. The connection between prepare-and-measure protocols and entanglement-based protocols will be discussed in more detail in a later material, as it is part of the security proof for the BB84 protocol.

Entanglement-based quantum key distribution involves the distribution of perfectly entangled states to generate a secure key. The protocol utilizes quantum error correction codes, such as the Calderbank-Shor-Steane code, to correct errors and ensure the security of the key.

In the entanglement-based quantum key distribution (QKD) protocol, Bob's role is to receive and measure the state sent by Alice. However, there is an alternative way to achieve the same result. This alternative method is based on entanglement.

To begin, Alice prepares a bipartite entangled state called Phi. This state is defined as a tensor product of Alice's quantum state, labeled X, and an orthonormal basis for Alice's system. The tensor product states are weighted with the square root of the probability distribution for each realization of X.

Alice then sends the second half of the entangled state to Bob. After receiving it, Bob measures the state with respect to the basis X. It can be shown that this procedure yields the same statistics as the prepared measure protocol.

On Alice's side, the probability of obtaining an outcome Y in the prepared measure protocol is given by the probability distribution of the classical random variable Px(Y). In the entanglement-based version, this probability can also be calculated using the measurement corresponding to the outcome Y. This is represented by the POVM element P(Y), which turns out to be the identity in Bob's system.

By performing the calculations, it can be shown that the probability of obtaining outcome Y is the same in both protocols. On Bob's side, the state he receives if Alice's outcome is Y can be calculated. In the prepare protocol, it is simply Phi with an index Y. In the entanglement-based protocol, the state after Alice's measurement is applied to Phi and normalized with the square root of the probability of Y.

In practice, it is not easy for Alice to create the exact quantum state required for the entanglement-based protocol. Additionally, there are security and noise concerns when distributing the state to Bob. However, mathematically, the same statistics can be achieved with both the prepare measure and entanglement-based protocols.

Entanglement-based protocols can yield the same statistics as prepare measure protocols in quantum key distribution. However, practical implementation poses challenges. In the next phase, classical post-processing will be discussed, including error estimation, error correction, and removal of Eve's information from the bit strings.

EITC/IS/QCF QUANTUM CRYPTOGRAPHY FUNDAMENTALS DIDACTIC MATERIALS
LESSON: ERROR CORRECTION AND PRIVACY AMPLIFICATION
TOPIC: CLASSICAL POST-PROCESSING

In this didactic material, we will focus on the classical post-processing part of a quantum key distribution protocol. After the quantum transmission phase, Alice and Bob each hold a bit string that is partially correlated and partially secret. The goal of classical post-processing is to perform parameter estimation, error correction, and privacy amplification to obtain a secure key.

The first step in classical post-processing is parameter estimation, where Alice and Bob estimate the error rate in their bit strings. This step helps them decide whether to continue with the protocol or abort and try again. Alice sends a small sample of her bit string to Bob, who compares it to history and estimates the error rate. The intuition here is that if the error rate of the sample is small, the error rate of the remaining bit strings is likely to be similar. This intuition can be mathematically proven using Chernoff-Hoeffding type bounds, which provide inequalities for bounding the error rate.

One useful inequality in this context is the Chernoff inequality. Suppose we have a set of n random variables, denoted as ki, with values 0 or 1. We can define the average of these random variables as the sum of all individual random variables divided by n. If we draw a sample without replacement from these random variables, denoted as Xj, we can similarly define the average of this sample. We define a quantity K as the difference between the total average and the sample average, and a value beta between 0 and 1. The Chernoff inequality states that the probability of the sample average being greater than or equal to the total average plus beta is exponentially small in the sample size n. This inequality helps improve the intuition that a small error rate in the sample implies a small error rate in the remaining bit strings.

After parameter estimation, the next step is error correction. The goal here is to make the bit strings held by Alice and Bob equal. This step involves applying error correction codes to correct any errors in the bit strings. After error correction, Alice and Bob hold partially secret keys, meaning they have the same strings, but an adversary may have partial knowledge of the key.

The final step in classical post-processing is privacy amplification. The goal of privacy amplification is to remove any knowledge an adversary may have about the key, making it completely secret and secure. This step ensures that the key can be used in applications like the one-time pad for secure communication.

Classical post-processing in quantum key distribution protocols involves parameter estimation, error correction, and privacy amplification. Parameter estimation helps estimate the error rate in the bit strings, while error correction aims to make the bit strings equal. Privacy amplification removes any knowledge an adversary may have about the key, ensuring its security. These steps are crucial for obtaining a secure key in quantum key distribution protocols.

In the context of parameter estimation in quantum cryptography, we begin by establishing some notation. Let lambda_n represent the error rate in the remaining n bits, and K denote the error rate in the sample bits. Additionally, lambda_max is the threshold for the sample error rate, above which the protocol is deemed invalid. We also introduce a constant, gamma.

Our main interest lies in the probability that the error rate in the remaining n bits, which Alice and Bob intend to use for key generation, exceeds the error rate observed in the sample bits plus gamma. Naturally, we want this probability to be small, as it represents an undesired event.

To bound this probability, we first introduce further notation. We denote Alice's key as K_a and Bob's key as K_b. We can divide the bit stream K_a into a part used for the sample and a part representing the remaining bits. The same division applies to K_b. The error rate in the remaining bits, longer n, is defined as the bitwise addition modulo 2 between Alice and Bob's respective keys. This operation yields 0 when the bit strings at a position are the same, and 1 when they differ. The absolute value represents the number of positions where the bit strings differ. A similar definition applies to the sample error rate.

Furthermore, we define the quantity nu as K divided by the total number of bits, n. This represents the ratio of the sample size to the total number of bits. The total error rate, lambda, can be expressed as a linear

combination of the sample error rate and the error rate in the remaining bits, using nu.

Moving on to probabilities, we employ Bayes' theorem. This theorem states that the probability of an event A conditioned on an event B is equal to the probability of event B conditioned on event A, multiplied by the probability of event A divided by the probability of event B. In our case, event A is that the error rate of the remaining bits is greater than or equal to the error rate of the sample bits plus gamma, while event B represents the error rate of the sample bits being less than or equal to lambda_max.

Applying this inequality, we obtain an upper bound on the quantity of interest. By considering the probability of event A divided by the probability of event B, we can find an upper bound on the numerator. Multiplying each quantity by nu preserves the inequality. Rearranging the inequality, we arrive at the probability of the error rate of the remaining bits being greater than or equal to nu times the error rate of the sample bits plus (1 - nu) times the error rate of the remaining bits, plus the constant gamma.

At this point, we can leverage Chernoff's inequality. The form of the linear combination matches the formulation of Chernoff's inequality. We have a sample of size n and the total error rate of the bit strings. Chernoff's inequality provides an upper bound on the probability that the error rate of the remaining bits exceeds the error rate of the entire string plus a small constant gamma.

By applying these mathematical concepts, we can establish bounds on the probability of the error rate in quantum cryptography, enabling us to assess the security and reliability of the protocol.

In the field of cybersecurity, specifically in the realm of quantum cryptography, error correction and privacy amplification are crucial steps in ensuring the security of communication between parties. In this didactic material, we will explore the fundamentals of error correction and privacy amplification in the context of classical post-processing.

To begin, let's first discuss the concept of error correction. Error correction is the process of rectifying errors that may occur during the transmission of information between two parties, Alice and Bob. The goal of error correction is to make Alice and Bob's bit strings equal while revealing minimal information to an eavesdropper, Eve. This is achieved through the use of error correction protocols, which encode information about Alice's bit string and allow Bob to estimate a guess of Alice's bits. It is important to note that error correction is a classical procedure and does not involve any quantum quantities.

There are various classical error correction protocols available, but the focus of our discussion lies in how we can verify the success of the error correction process. To address this, we employ a concept called "two Universal hash functions." These functions, denoted as F, are defined as a family of functions that map inputs from an alphabet X to an alphabet Z. The family of functions is associated with a probability distribution, denoted as PS, which determines the likelihood of selecting a particular function from the family.

For a family of functions to be considered "two Universal," the probability that the output of the function applied to one input, X, is equal to the output of the function applied to another input, X prime, must be smaller or equal to 1 divided by the cardinality of the alphabet. This condition holds true only when the inputs, X and X prime, are not equal, and the function F is randomly chosen from the family according to the given probability distribution PF. In simpler terms, this means that the probability of two different inputs producing the same output is very small, especially when the alphabet set is large.

The significance of two Universal hash functions lies in their ability to detect errors without revealing the actual values of the bit strings. Alice and Bob can compare the outputs of these functions and determine if they are equal. If the outputs are equal, they can be confident that the inputs were also the same. This checking procedure ensures the success of the error correction process.

Moving on to privacy amplification, this step is undertaken to further enhance the security of the communication between Alice and Bob. Privacy amplification involves the reduction of any remaining information that an eavesdropper, Eve, may possess about Alice and Bob's bit strings. This is achieved by applying a cryptographic hash function to the bit strings, which transforms them into shorter, uniformly random strings. The resulting strings are then used as secure keys for subsequent cryptographic operations.

Error correction and privacy amplification are vital components of classical post-processing in quantum

cryptography. Error correction ensures that Alice and Bob's bit strings are made equal while minimizing the information revealed to an eavesdropper. Privacy amplification, on the other hand, further enhances the security of the communication by reducing any remaining information that an eavesdropper may possess. By employing the concept of two Universal hash functions and cryptographic hash functions, the integrity and confidentiality of the communication can be ensured.

In the field of quantum cryptography, error correction and privacy amplification are crucial steps in ensuring the security of key transmission. After the error correction process, some information about the key may have been leaked to an eavesdropper, referred to as Eve. Therefore, it is necessary to remove Eve's knowledge of the key to achieve secure communication.

To accomplish this, a randomness extractor is used. A randomness extractor is a function that takes as input a source of randomness, which in this case is a bit string, and a small uniformly random string called the seed. It then outputs an almost uniformly random string that is longer than the seed. However, there are certain requirements for the randomness extractor to be effective.

Firstly, the output string should be independent of the seed, as the seed may not be necessary to communicate. This requirement is covered by the term "strong randomness extractor." Secondly, the randomness extractor should take into account the presence of a quantum adversary, such as Eve, who has some knowledge about the key. This is captured by the term "quantum-proof strong randomness extractor."

In the context of error correction and privacy amplification, we focus on Alice's system. Alice holds a bit string, which is represented by a classical random variable X. Eve, the quantum adversary, is described by a quantum system denoted as E. The state of the composite system of Alice and Eve can be described by a classical-quantum system, denoted as ρ_{XE}. The classical-quantum system consists of states of an orthonormal basis X that encode the classical bits, with each state described by a quantum state ρ_E indexed by X, weighted by the probability distribution p_X of X.

Additionally, there is a system that describes the seed, denoted as ρ. The actual state of the seed is not important; what matters is that the final key is independent of the seed. To quantify Eve's information, we use the quantum conditional min entropy. This entropy measures the amount of uncertainty in the key given Eve's knowledge.

The quantum conditional min entropy of a bipartite state $\rho_{A B}$, conditioned on the system B, is defined as follows: We seek a parameter λ that satisfies the inequality $\rho_{A B} \leq \lambda I_A \otimes \sigma_B$, where σ_B is a state of system B. The set of all parameters that satisfy this equation for a given state σ_B is denoted as $\Lambda(\sigma_B)$. We are interested in the minimum value of λ over all possible states σ_B, and then we take the negative logarithm of this value.

Although the definition of quantum conditional min entropy may seem technical, its operational interpretation aligns with our goal. In the context of classical-quantum states, the quantum conditional min entropy characterizes the amount of uniform randomness that can be extracted from the classical random variable correlated with the quantum system.

Error correction and privacy amplification are essential steps in quantum cryptography. By employing a randomness extractor and quantifying Eve's information using the quantum conditional min entropy, it is possible to remove Eve's knowledge of the key and achieve secure communication.

In the field of quantum cryptography, error correction and privacy amplification are crucial steps in ensuring the security and reliability of quantum communication protocols. In this didactic material, we will explore the fundamentals of error correction and privacy amplification in the context of classical post-processing.

To begin, let's first understand the concept of quantum proof strong randomness extractors. These extractors are functions that take as input a bit string of length n and a bit string of length D, and output a bit string of length M. The goal of a quantum proof strong randomness extractor is to ensure that for all classical or quantum states with a minimum entropy $H_{min}(X|Y)$ greater than or equal to a parameter K, and a uniform random seed Y, the trace distance between the state after applying the randomness extractor and the maximally mixed state is smaller than or equal to another parameter Epsilon.

The trace distance, denoted as ||Rho1 - Rho2||, is a measure of the difference between two quantum states. It is defined as the trace of the square root of the product of the conjugate transpose of Rho1 and Rho1. In other words, it quantifies the distinguishability of two quantum states.

The quantum conditional min entropy, Hmin(X|Y), characterizes the amount of information that an eavesdropper, Eve, has about the input string X given the seed Y. It is important to have a lower bound on this entropy, as it indicates the amount of uniform randomness that can be extracted. If the entropy is zero, it means that no randomness can be extracted to fulfill the required security requirements.

Now, let's move on to the practical implementation of error correction and privacy amplification. One example of a quantum proof strong randomness extractor is the use of two Universal hash functions. In this approach, Alice and Bob, the communicating parties, both have access to these hash functions. Alice randomly selects a function from the family of two Universal hash functions using a seed. She applies this function to her input string and announces her choice to Bob. Bob applies the same function to his input string. After this step, Alice and Bob hold identical key strings that are independent of each other's systems.

The classical post-processing involves three main steps. Firstly, Alice and Bob estimate the error rate to determine if it is worth continuing with the protocol. Secondly, they perform error correction to transform their partially secret correlation into a partially secret key. This step ensures that they hold identical key strings while having some information on the errors. Finally, they perform privacy amplification to further enhance the security of the key. Privacy amplification involves applying a function to the key strings to remove any residual information that an eavesdropper may possess.

Error correction and privacy amplification are essential steps in classical post-processing for quantum communication protocols. These steps ensure the security and reliability of the shared key between Alice and Bob. By estimating the error rate, performing error correction, and applying privacy amplification techniques, Alice and Bob can establish a secure and secret key that can be used for various applications.

In quantum cryptography, the goal is to establish secure keys between two parties, Alice and Bob, by taking advantage of the principles of quantum mechanics. In the previous material, we discussed the protocols used for quantum key distribution. Now, let's delve deeper into the concept of security in these protocols.

When we talk about security in quantum cryptography, we mean that the keys generated should be secure against any eavesdropping attempts by an adversary, Eve. In other words, Eve should not be able to gain any knowledge about the secret keys shared between Alice and Bob.

To ensure security, quantum cryptography protocols employ various techniques, such as error correction and privacy amplification. Error correction is a process where errors that occur during the transmission of quantum bits, or qubits, are detected and corrected. This is crucial because any errors in the received qubits could potentially leak information to Eve.

Privacy amplification, on the other hand, is a process that further reduces the amount of information that Eve could potentially obtain. It involves extracting a smaller, but more secure, key from the partially secret key obtained through the error correction process.

In addition to error correction and privacy amplification, classical post-processing is also an important aspect of ensuring security in quantum cryptography protocols. Classical post-processing involves performing additional computations on the shared key to enhance its security. This can include techniques such as hashing, randomization, and authentication.

By employing these techniques, quantum cryptography protocols aim to establish secure keys that are resistant to attacks by Eve. In the forthcoming material, we will discuss the security of specific protocols and explore different strategies to prove their security, diving deeper into the security aspects of quantum cryptography.

EITC/IS/QCF QUANTUM CRYPTOGRAPHY FUNDAMENTALS DIDACTIC MATERIALS
LESSON: SECURITY OF QUANTUM KEY DISTRIBUTION
TOPIC: SECURITY DEFINITION

This part of the material is currently undergoing an update and will be republished shortly.

EITC/IS/QCF QUANTUM CRYPTOGRAPHY FUNDAMENTALS DIDACTIC MATERIALS
LESSON: SECURITY OF QUANTUM KEY DISTRIBUTION
TOPIC: EAVESDROPPING STRATEGIES

Quantum key distribution (QKD) is a method used in cybersecurity to establish secure communication channels. In the previous material, we discussed how to design a secure QKD protocol to protect against eavesdropping attacks. Now, we will delve into the specific eavesdropping strategies that an attacker, known as Eve, can employ to gain information about the key.

Before we explore the eavesdropping strategies, let's consider an important aspect: how much disturbance does Eve need to introduce to the quantum states in order to gain information? If Eve could obtain information without disturbing the states, it would be undetectable. To analyze this, we will focus on the BB84 protocol, which involves the states 0 and 1 in the computational basis, as well as their corresponding states in the Hadamard basis.

The most general attack that Eve can perform is attaching an ancillary state to the state sent by Alice, applying a unitary transformation to the composite system, and then measuring her part of the system. By doing this, Eve aims to obtain information without disturbing Alice's state. We denote the attached ancillary state as "e" in our analysis.

When Eve performs this attack, the only change occurs in her state, while Alice's state remains undisturbed. We compare the scalar product of the states before and after the unitary transformation. By analyzing this, we can make an important observation about the states held by Eve after the transformation.

If the initial states sent by Alice are not orthogonal (meaning their scalar product is not zero), we can conclude that the states held by Eve after the unitary transformation must be the same. This implies that, regardless of the initial state prepared by Alice, Eve always obtains the same state in her system after the transformation. However, since the two states held by Eve are identical, no information about Alice's system can be gained from these states. In order to obtain information, the two states in Eve's ancillary system must be distinguishable, which is not the case here.

This result is favorable because it means that if Eve chooses to use a unitary transformation that does not disturb Alice's states, she cannot gain any information about the key. However, if Eve wants to gain information, she must disturb Alice's states.

Let's now examine the scenario where Eve needs to disturb the system. In this case, both Alice's and Eve's states change after the unitary transformation. We analyze the scalar product of the states before and after the transformation, taking into account the changes introduced.

By comparing the left-hand side and the right-hand side of the equation, we observe that the right-hand side consists of two terms: the scalar product of Alice's states after the transformation and the scalar product of the disturbed states. The disturbed states are denoted as "0'1'" to signify the changes introduced.

From this analysis, we can conclude that when Eve disturbs the system, the scalar product of Alice's states after the transformation is no longer equal to 1. This implies that the scalar product of the disturbed states is not equal to 1 either. Therefore, the two states held by Eve after the transformation are different, depending on the initial state prepared by Alice.

This difference in states held by Eve allows her to gain information about Alice's system. By measuring her part of the system, Eve can obtain information about the key. However, this also means that Eve's attack can be detected, as the disturbance introduced by her actions is detectable.

In order to gain information about the key in quantum key distribution, an eavesdropper must disturb the quantum states. If the eavesdropper chooses a unitary transformation that does not disturb Alice's states, no information can be obtained. However, if the eavesdropper introduces disturbance, information can be gained, but the attack becomes detectable.

In the field of cybersecurity, quantum cryptography plays a crucial role in ensuring the security of

communication systems. One fundamental aspect of quantum cryptography is the security of quantum key distribution, which involves protecting the transmission of cryptographic keys using quantum principles.

When it comes to the security of quantum key distribution, one of the main concerns is eavesdropping. Eavesdropping refers to the unauthorized interception of communication between two parties. In the context of quantum key distribution, an eavesdropper, often referred to as Eve, tries to gain information about the cryptographic key being transmitted.

In order to understand the strategies employed by eavesdroppers, it is important to consider the distinguishability of quantum states. In quantum key distribution, each quantum state needs to be distinguishable in order to extract information about the state. The more distinguishable the states are, the more information Eve can obtain about the cryptographic key. To minimize the amount of information Eve can gain, the scalar product of the ancillary states used by Eve should be as small as possible. If the scalar product is zero, it means the states are orthogonal, allowing perfect information about the cryptographic key. However, there is a trade-off between information gain and disturbance introduced to the states. As Eve gains more information, she also introduces more disturbance, making her attack more easily detectable.

Now, let's discuss the general classification of eavesdropping strategies. There are three main types: individual attacks, collective attacks, and coherent attacks.

In individual attacks, each state that Alice sends is attacked individually and in the same way. The ancillary state used by Eve after the attack is described by attaching an ancillary state to Alice's state, performing a unitary operation on the composite system, and then tracing out Alice's system. The measurement is performed individually on each state, resulting in a probability distribution that corresponds to the individual probabilities for each state.

In collective attacks, the measurement is performed globally over all the ancillary states that Eve collects. Similar to individual attacks, an ancillary state is attached to each of Alice's states, and a unitary operation is performed on the composite system. However, the measurement is done collectively for all the ancillary states that Eve has. This results in a probability distribution that acts on multiple states.

Coherent attacks are the most powerful and general type of eavesdropping strategy. In coherent attacks, the entire set of states that Alice sends is attacked as a global system. This allows Eve to obtain the most information but also makes the attack more difficult to execute. The ancillary state used by Eve and the resulting probability distribution depend on the specific coherent attack strategy employed.

Eavesdropping strategies in quantum key distribution can be classified into individual attacks, collective attacks, and coherent attacks. Each strategy has its own characteristics and implications for the security of the cryptographic key being transmitted. Understanding these strategies is crucial for developing robust quantum cryptography protocols.

Quantum cryptography is a field of study that focuses on using quantum mechanics principles to ensure secure communication. One important aspect of quantum cryptography is the security of quantum key distribution (QKD) protocols. In this didactic material, we will explore the concept of eavesdropping strategies and their impact on the security of QKD.

There are three different classes of attacks that an eavesdropper, also known as Eve, can employ: individual attacks, coherent attacks, and collective attacks. Individual attacks are the easiest to analyze because they involve looking at only one state at a time. Eve performs a unitary transformation on the state sent by Alice and measures the outcome. The probability distribution of the measurement results is determined by the initial state and the disturbance introduced by Eve. The fidelity, which measures the closeness between quantum states, is used to quantify the disturbance introduced by Eve.

Coherent attacks are more complex because they involve a larger Hilbert space. The dimension of the Hilbert space grows rapidly with the number of states sent by Alice. Analyzing coherent attacks requires considering the unitary transformation and the measurement performed by Eve. The resulting state received by Bob is a linear combination of 0 and 1 states, with coefficients determined by the fidelity between the input and output states.

Collective attacks are the most powerful, but also the most challenging to analyze. In these attacks, Eve attaches an ancilla state to the state sent by Alice and performs a global unitary transformation on the composite system. The resulting state received by Bob is a linear combination of 0 and 1 states, with coefficients determined by the fidelity and the initial state.

To evaluate the security of QKD protocols, researchers analyze the mutual information between Alice and Bob, which represents the amount of information that Eve can potentially obtain. For the BB84 protocol, the mutual information between Alice and Bob, as well as the mutual information between Alice and Eve, can be calculated using formulas derived from the fidelity. Similarly, for the 6-state protocol, the mutual information between Alice and Bob remains the same as in the BB84 protocol, while the mutual information between Alice and Eve changes.

To gain a better understanding of how the mutual information varies for different protocols, plots of the mutual information are often used. These plots show how the mutual information between Alice and Bob and Alice and Eve changes as the disturbance introduced by Eve varies.

Eavesdropping strategies play a crucial role in the security of quantum key distribution protocols. By analyzing individual, coherent, and collective attacks, researchers can assess the potential information leakage and evaluate the security of QKD protocols.

In the field of cybersecurity, one of the fundamental concepts is quantum cryptography, which aims to ensure secure communication by utilizing the principles of quantum mechanics. One crucial aspect of quantum cryptography is the security of quantum key distribution (QKD), which involves the exchange of cryptographic keys between two parties, Alice and Bob, using quantum states.

However, an important concern in QKD is the possibility of eavesdropping, where an unauthorized third party, Eve, tries to intercept and gain access to the exchanged key. In order to understand the strategies employed by eavesdroppers, it is essential to analyze the mutual information between Alice and Eve, as well as between Alice and Bob.

The mutual information represents the amount of information shared between two parties. In the case of QKD, the goal is to maximize the mutual information between Alice and Eve, as this indicates the effectiveness of eavesdropping. On the other hand, Alice and Bob aim to minimize the mutual information between them and Eve, as this ensures the secrecy of the key.

By analyzing the mutual information, it becomes evident that as the disturbance introduced by Eve increases, the mutual information between Alice and Eve also increases. This holds true for both protocols, namely the VB 84 and the 6-state protocol. However, as the disturbance increases, the mutual information between Alice and Bob decreases, which raises suspicion.

Furthermore, when the mutual information between Alice and Eve surpasses the mutual information between Alice and Bob, it becomes impossible for Alice and Bob to extract the secret key from the state. This point marks the threshold beyond which no secret key can be extracted.

Comparing the VB 84 and the 6-state protocol, it can be observed that the mutual information between Alice and Eve is slightly higher for the 6-state protocol. However, the advantage of the 6-state protocol lies in the fact that for individual attacks, the mutual information between Alice and Eve is lower. This means that the 6-state protocol can withstand a slightly higher disturbance before the point of no secret key extraction is reached.

To provide a clearer understanding, the difference between the mutual information of Alice and Bob and the mutual information of Alice and Eve is plotted. This graph shows that the point of equality, beyond which no secret key can be extracted, is reached slightly earlier for the VB 84 protocol compared to the 6-state protocol.

Moving on to coherent attacks, it is important to note that they pose a greater challenge due to the high dimensionality of the global Hilbert space in QKD protocols. Coherent attacks involve exploiting the global properties of the quantum states exchanged between Alice and Bob.

Although analyzing coherent attacks is more complex, some studies have been conducted. For the VB 84 and the 6-state protocol, it has been observed that the probability of Eve gaining more information on the individual

key bits does not increase significantly when using a coherent attack instead of individual attacks. However, the probability of correctly guessing the entire message slightly increases with a coherent attack.

An analysis of coherent attacks for the VB 84 protocol revealed that the probability of both Bob and Eve correctly guessing the message slightly increased compared to individual attacks. Similar investigations for the 6-state protocol yielded the same conclusion, indicating that coherent attacks do not provide additional information on the individual bits, but increase the probability of correctly guessing the entire message.

In addition to individual and coherent attacks, another important aspect to consider is the vulnerability of certain protocol implementations. One such attack is the photon number splitting attack, which targets specific implementations of the protocol. Understanding these attacks is crucial for identifying potential vulnerabilities and improving the security of QKD protocols.

The analysis of eavesdropping strategies in quantum cryptography involves examining the mutual information between Alice and Eve, as well as between Alice and Bob. The goal is to maximize the mutual information for eavesdroppers while minimizing it for the legitimate parties. Coherent attacks pose a greater challenge due to the high dimensionality of the global Hilbert space. Furthermore, it is important to consider specific attacks, such as the photon number splitting attack, to enhance the security of protocol implementations.

Quantum cryptography is a field of study that focuses on developing secure communication protocols using the principles of quantum mechanics. One of the fundamental aspects of quantum cryptography is the security of quantum key distribution (QKD), which ensures that the keys exchanged between two parties, Alice and Bob, are secure from eavesdroppers.

To implement QKD, we need qubits, which are the basic units of quantum information. In practice, qubits can be realized using photons. However, perfect single photon sources are not readily available. Instead, coherent laser pulses are used as approximate single photon sources. These laser pulses have a specific form, denoted by alpha, which represents the phase of the laser. The state of a laser pulse can be described as an infinite sum over the number of photons it contains, denoted by n. When the phase of the laser is unknown or randomized, it results in a phase-randomized coherent state, which is a sum over the number states with a Poisson distribution.

The average photon number, denoted by mu, is an important parameter in laser pulses. In practice, a typical laser pulse has an average photon number of 0.1. This means that most of the pulses sent by Alice will be vacuum events, where no photons are present. Single photon events, which are crucial for the implementation of the protocol, occur with a probability of about 9%. These events are similar to those produced by a perfect single photon source. However, there are also multiphoton events, which occur with a probability of 0.5%. These events can be exploited by an eavesdropper, Eve, to perform a photon number splitting attack.

The photon number splitting attack involves Eve performing a non-destructive measurement on the pulses sent by Alice to determine the number of photons present. If there is more than one photon, Eve can split off one photon and forward the rest to Bob. She can then store the split-off photon and wait for Alice to reveal her basis choice for the photons. By performing the correct measurement, Eve can gain perfect information on this part of the key without being detected.

In practice, the quantum channel used for communication is not perfect and has some losses, characterized by the transmittivity, denoted by eta. The average detected photon number is given by the product of the transmittivity and the average photon number of the laser pulse. This means that the probability of Bob detecting a photon, rather than a vacuum, is 1 - e^(-mu*eta), due to the Poisson distribution.

Eve's goal is to perform an attack that cannot be detected, so she replaces the lossy quantum channel with a perfect one, where every photon is transmitted. However, she needs to ensure that the probability of Bob detecting a photon remains unchanged. She has different options for dealing with the different events that can occur, including vacuum events, single photon events, and multiphoton events. Vacuum events are simply forwarded, as they provide no information. Single photon events are crucial for the protocol and are used by Alice and Bob. Multiphoton events are the ones that Eve can exploit for the photon number splitting attack.

The security of quantum key distribution relies on the use of qubits, specifically photons, to implement the protocol. Coherent laser pulses are used as approximate single photon sources, and the average photon number

is an important parameter. While vacuum and single photon events are used for the protocol, multiphoton events can be exploited by an eavesdropper to perform a photon number splitting attack. Understanding these concepts is essential for ensuring the security of quantum key distribution.

In the previous material, we discussed various eavesdropping strategies that an attacker, referred to as Eve, can employ to compromise the security of quantum key distribution. One such strategy is known as the coherent attack, where Eve splits a photon and forwards the remaining photons to the intended recipient, Bob. Eve then performs a coherent attack on these photons, attempting to extract information without being detected. However, this attack introduces errors to the system, potentially compromising the security of the quantum key.

To counter this coherent attack, a possible solution is the S-ARG protocol, which involves Alice and Bob using different types of sifting to avoid revealing the bases. By doing so, Eve's ability to gather information is significantly limited, making the attack less effective.

Another countermeasure against eavesdropping is the use of decoy states. In this strategy, Alice incorporates a second source of weak coherent pulses, referred to as the decoy source, with a higher mean photon number. During the transmission, Alice randomly inserts decoy states between the signal states. Since Eve cannot distinguish between the two types of states, she performs her attack on all of them. However, this also means that she cannot accurately estimate the average photon number for both sources. At the end of the transmission, Alice reveals which states were decoyed, and Bob can then compare the observed loss in signal states to the expected loss. If the observed loss is significantly higher than expected, it indicates the presence of Eve's attack.

By implementing these countermeasures, the security of quantum key distribution can be enhanced, making it more resilient against eavesdropping attempts. In the next material, we will delve into the security of the VBAT4 protocol.

EITC/IS/QCF QUANTUM CRYPTOGRAPHY FUNDAMENTALS DIDACTIC MATERIALS
LESSON: SECURITY OF QUANTUM KEY DISTRIBUTION
TOPIC: SECURITY OF BB84

This part of the material is currently undergoing an update and will be republished shortly.

EITC/IS/QCF QUANTUM CRYPTOGRAPHY FUNDAMENTALS DIDACTIC MATERIALS
LESSON: SECURITY OF QUANTUM KEY DISTRIBUTION
TOPIC: SECURITY VIA ENTROPIC UNCERTAINTY RELATIONS

This part of the material is currently undergoing an update and will be republished shortly.

EITC/IS/QCF QUANTUM CRYPTOGRAPHY FUNDAMENTALS DIDACTIC MATERIALS
LESSON: PRACTICAL QUANTUM KEY DISTRIBUTION
TOPIC: QKD - EXPERIMENT VS. THEORY

This part of the material is currently undergoing an update and will be republished shortly.

EITC/IS/QCF QUANTUM CRYPTOGRAPHY FUNDAMENTALS DIDACTIC MATERIALS
LESSON: PRACTICAL QUANTUM KEY DISTRIBUTION
TOPIC: INTRODUCTION TO EXPERIMENTAL QUANTUM CRYPTOGRAPHY

This part of the material is currently undergoing an update and will be republished shortly.

EITC/IS/QCF QUANTUM CRYPTOGRAPHY FUNDAMENTALS DIDACTIC MATERIALS
LESSON: PRACTICAL QUANTUM KEY DISTRIBUTION
TOPIC: QUANTUM HACKING - PART 1

This part of the material is currently undergoing an update and will be republished shortly.

EITC/IS/QCF QUANTUM CRYPTOGRAPHY FUNDAMENTALS DIDACTIC MATERIALS
LESSON: PRACTICAL QUANTUM KEY DISTRIBUTION
TOPIC: QUANTUM HACKING - PART 2

This part of the material is currently undergoing an update and will be republished shortly.

EITC/IS/QCF QUANTUM CRYPTOGRAPHY FUNDAMENTALS DIDACTIC MATERIALS
LESSON: PRACTICAL QUANTUM KEY DISTRIBUTION
TOPIC: QKD TEACHING KIT

In this didactic material, we will explore the fundamentals of quantum cryptography, focusing on practical quantum key distribution (QKD) using the BB84 protocol, as well as Quantum Cryptography educational kits.

Encryption is a crucial aspect of secure communication. Traditionally, encryption involves encoding a message or image using a key through bitwise addition. However, ensuring safe communication is a challenge. Quantum cryptography offers a solution by providing secure communication through the use of quantum mechanical principles.

The one-time pad is an example of a secure encryption method. It requires three prerequisites. First, the key must be secret, known only to the sender and receiver. Second, the key should be used only once and be long enough to encrypt the entire message. Using the key multiple times or having a short key compromises security. Third, the key must be completely random, making it resistant to attacks. Generating truly random keys is essential for secure communication.

Quantum physics plays a role in achieving secure communication in two ways. The first is ensuring that the key is known only to the sender and receiver. This is achieved through the BB84 protocol, which we will discuss in detail. The second is the use of quantum randomness to generate the key. Quantum mechanics provides inherently random processes that can be utilized for secure encryption.

The BB84 protocol involves two parties, Alice (the sender) and Bob (the receiver), generating a tamper-proof key together. The key generation process is what makes it secure against eavesdropping. Eve, the eavesdropper, attempts to intercept the key generation and data transmission. However, the design of BB84 ensures that any interference from Eve leaves a trace that can be detected by Alice and Bob. This detection mechanism guarantees the security of the key generation process.

Once the tamper-proof key is generated, the encrypted message can be transmitted publicly. If all the prerequisites mentioned earlier are met, the encrypted message contains no information that can be exploited. The key is completely random and known only to Alice and Bob, ensuring the security of the communication.

The Quantum Cryptography Educational Kit provides a setup that allows one to explore all the steps of the BB84 protocol. The kit goes beyond using single photons for encoding. We delve into the relationship between classical and quantum mechanical aspects, highlighting how this knowledge enhances the teaching experience.

By using the kit, you can gain hands-on experience with quantum cryptography and understand the practical implementation of quantum key distribution.

In the field of Quantum Cryptography, one of the fundamental concepts is Quantum Key Distribution (QKD). QKD allows secure communication between two parties by using the principles of quantum mechanics. In this teaching kit, we will focus on the practical implementation of QKD using the BB-84 protocol.

To understand the setup, we have three parties involved: Alice (the sender), Bob (the receiver), and Eve (the potential eavesdropper). The setup consists of two breadboards, one for Alice and one for Bob, with the option to include Eve in between them. The goal is to transmit data securely between Alice and Bob, while detecting any presence of Eve.

The first step in the process is to prepare the polarization state of the light that Alice wants to send. This is achieved by using a laser on Alice's breadboard, which is linearly polarized. The laser can be operated in two modes: continuous wave for system alignment and short pulse for data transmission. It's important to note that in this educational kit, we are using short laser pulses as an analogy for single photons. While it's not a true quantum optics kit, the principles and concepts can still be effectively taught using this setup.

Alice's breadboard also includes a half-wave plate, which allows her to set a specific polarization orientation or state. The plate has two different states, corresponding to two different measurement bases: the x basis and the plus basis. In the x basis, the polarization states are -45 degrees and +45 degrees, representing digital zero

and one, respectively. In the plus basis, the polarization states are 0 degrees and 90 degrees, also representing digital zero and one. These polarizations are referred to as vertical and horizontal, respectively.

Moving on to Bob's breadboard, he also has a half-wave plate that serves a similar purpose. The light from Alice's setup reaches Bob's breadboard through a polarizing beam splitter. Depending on the orientation of Bob's half-wave plate, the light can either be transmitted or reflected. The transmitted path is labeled as zero, and the reflected path is labeled as one. Bob's choice of measurement basis, either the plus basis or the x basis, determines the orientation of his half-wave plate (0 degrees or 45 degrees).

Bob's breadboard also includes two photo detectors, one for each path. These detectors have LEDs that light up when a laser pulse is detected. This visual feedback helps in understanding where the photon is detected.

To illustrate the process, let's consider a few examples. When Alice sends a digital zero in the plus basis, the half-wave plate on her breadboard is set at 0 degrees. If Bob also measures in the plus basis, his half-wave plate remains at 0 degrees, and the LED on the corresponding photo detector lights up, indicating the detection of the photon.

Similarly, when Alice wants to send a digital one in the x basis, the half-wave plate on her breadboard is rotated to 45 degrees. If Bob measures in the x basis as well, the LED on the corresponding photo detector lights up.

The interesting case arises when Alice wants to send a digital one in the x basis, but Bob measures in the plus basis. In this scenario, the outcome is different, and this is where the presence of Eve can be detected. The specifics of this case were not mentioned in the transcript.

This teaching kit provides a practical demonstration of Quantum Key Distribution using the BB-84 protocol. The setup involves Alice and Bob with their respective breadboards, and the option to include an eavesdropping unit, Eve. By manipulating the polarization states of light and measuring them in different bases, secure communication can be achieved while detecting any potential eavesdropping attempts.

Let's reiterate exploration of the practical implementation of QKD using the BB-84 protocol. A photon with a 45-degree orientation enters a polarizing beam splitter. This splitter allows photons with a 0-degree orientation to transmit and reflects photons with a 90-degree orientation. In the case of a single photon, it randomly decides which path to take. However, in our setup, we are dealing with laser pulses, so the intensity of the pulse is split in half. To maintain randomness, a random mode is integrated into the sensor electronics box. This ensures that the intensity reaching the photodiodes is equal, indicating a mismatch of bases, and randomly lights up either of the LEDs.

Now, let's demonstrate the different cases. First, in the continuous wave mode, used for system alignment, both Alice and Bob set their half-wave plates to a 0-degree orientation. When a pulse is sent, the LED indicating a 0-degree measurement lights up. In the next case, Alice wants to send a 45-degree photon, and Bob measures in the same basis. When the pulse is sent, the LED indicating a 1 lights up. These are the cases where the bases match.

Now, let's consider a case where the bases do not match. Alice sends a 45-degree photon, but Bob measures in the 0-degree basis. In this case, the result is random, and either LED can light up.

Now that we have seen the setup and the different cases, let's dive into the details of the BB-84 protocol and how it is reproduced in our setup. To generate the key, Alice chooses random bases and bits. This can be represented in a table, assuming 18 measurements. Alice fills the table with bases and bits. It is important to note that quantum physics plays a crucial role here, as we require truly random bases and bits.

As an educational exercise, one can be asked to generate a series of random zeros and ones. By analyzing the distribution of different string lengths, it becomes evident that humans are not good random number generators. This serves as a practical demonstration of the need for quantum randomness. One can for example provide learners with a number of dices to ensure random bases and bits.

Quantum Key Distribution is a powerful tool in ensuring secure communication. By implementing the BB-84 protocol, we can generate a secure key between two parties. Understanding the principles behind quantum randomness and its practical implementation is essential in the field of quantum cryptography.

To summarize the BB84 protocol, Alice and Bob each have a set of randomly chosen bases, which are used to measure the polarization of quantum particles, typically photons. The two parties agree on four possible bases: X, +, /, and \. The X basis represents the horizontal-vertical polarization, while the +, /, and \ bases represent diagonal polarizations.

The process begins with Alice preparing a series of quantum particles, each in a random polarization state, according to the chosen bases. She then sends these particles to Bob through a quantum channel. Bob also randomly chooses a basis for each particle he receives.

During the measurement phase, Alice and Bob compare their chosen bases for each particle. They do this by communicating the basis information over a public channel, which is assumed to be secure. By comparing the bases, they can determine whether the measurement results are reliable or random.

If Alice and Bob used the same basis for a particular measurement, they keep the corresponding bit as part of their shared key. If their bases do not match, they discard the measurement result. This process ensures that only bits measured with matching bases contribute to the shared key.

After going through all the measurements, Alice and Bob have a set of matching bits, which form their shared secret key. This key can then be used for encryption and decryption of messages between the two parties.

It is important to note that the security of QKD lies in the principles of quantum mechanics. Any attempt to eavesdrop on the quantum channel would disturb the particles, causing errors in the measurement results. This would be detected by Alice and Bob during the basis comparison phase, ensuring the security of the key.

QKD is a practical implementation of quantum cryptography that allows two parties, Alice and Bob, to establish a shared secret key for secure communication. The BB84 protocol is one example of a QKD scheme, where random bases are chosen, quantum particles are measured, and the basis information is compared to generate a shared key. This key can then be used for secure encryption and decryption of messages.

Quantum cryptography is a powerful tool in ensuring secure communication by leveraging the principles of quantum mechanics. One of the fundamental concepts in quantum cryptography is Quantum Key Distribution (QKD), which allows two parties, Alice and Bob, to establish a secret key that can be used for secure communication. In this didactic material, we will focus on the practical implementation of QKD and how it addresses the issue of eavesdropping.

To understand the practical implementation of QKD, it is important to introduce the concept of an eavesdropper, represented by Eve. In a QKD system, an eavesdropper can intercept the quantum signals being transmitted between Alice and Bob. The BB-84 protocol, a widely used QKD protocol, is particularly effective in detecting the presence of an eavesdropper.

An eavesdropping unit can be introduced to simulate Eve's presence. This unit consists of measurement units similar to those used by Bob. It includes a half-wave plate to choose the measurement bases, a polarizing beam splitter, and two detectors. Eve's goal is to measure the quantum state of the transmitted photons and relay that information to Bob without being detected.

The detection of Eve is based on the fact that any measurement in quantum mechanics alters the quantum state. When Alice and Bob measure in different bases, the measurements are discarded, making it uninteresting for Eve. However, when all three parties choose the same bases, interesting scenarios arise.

Let's consider a scenario where Alice wants to send a digital one in the x basis. She sends a photon with a 45-degree orientation. If Eve measures in the same basis, she will get the 45-degree orientation, and the detector will light up. Eve then relays this information to Bob, who also measures in the same basis and gets the digital one. In this case, Eve's presence is not detected, as all bases match.

Now, let's consider the scenario where Eve measures in a different basis than Alice and Bob. Again, Alice wants to send a digital one in the x basis. If Eve measures in the plus basis, the result is random. Let's assume she measures a zero. Eve then sends the zero-degree polarized photon in the same basis. Bob, however, measures in the x basis, and the result is also random. It could be a one or a zero. If Bob measures a zero, this is the

interesting case where Eve is detected. Despite the matching bases, the results do not match, indicating the presence of an eavesdropper.

It is important to note that Alice and Bob compare a number of test bits after generating a long key. This is where they can detect if someone has listened in on the key generation process. Through mathematical analysis, it is determined that 25% of the test bits will feature a false result if an eavesdropper is present. This indicates that someone has intercepted the key generation process, not the actual message encryption and transmission.

The practical implementation of QKD involves detecting the presence of an eavesdropper by comparing measurement results. The BB-84 protocol is particularly effective in this regard. By comparing test bits, Alice and Bob can determine if their key generation process has been compromised. This ensures that the secure message transmission is protected from unauthorized interception.

In the field of cybersecurity, quantum cryptography has emerged as a promising solution to enhance the security of communication systems. One important aspect of quantum cryptography is practical quantum key distribution (QKD), which allows secure exchange of cryptographic keys between two parties, typically referred to as Alice and Bob. In this didactic material, we will explore the fundamentals of QKD and understand how it can be implemented in a practical setting.

QKD relies on the principles of quantum mechanics to ensure the security of the exchanged keys. Unlike classical encryption methods, which can be compromised by advanced computational algorithms, QKD provides a provably secure method for key distribution. The security of QKD is based on the fundamental properties of quantum states, such as the no-cloning theorem and the uncertainty principle.

To understand the concept of QKD, let's consider a scenario where Alice wants to securely communicate with Bob. They both have access to a quantum communication channel, which can be implemented using optical fibers or other quantum systems. The goal is to establish a shared secret key that can be used for subsequent encryption and decryption of messages.

In QKD, the key distribution process involves the exchange of quantum states, typically photons, between Alice and Bob. These photons carry the information that will be used to generate the shared key. The key distribution process consists of several steps, including key generation, key reconciliation, and key confirmation.

During the key generation step, Alice prepares a sequence of quantum states, typically using a laser pulse, where each state represents a bit of the key. For example, a "0" bit can be represented by the absence of a photon, while a "1" bit can be represented by the presence of a photon. Alice randomly chooses the basis in which each state is prepared, such as the x-basis or the plus-basis.

Bob, on the other hand, randomly chooses the basis in which he measures the received states. The measurement basis can be the same as Alice's or different. After the measurement, Alice and Bob publicly announce their chosen bases for each state. They then compare a subset of their measurement results to check for any discrepancies. If the bases match, they expect the measured bits to be the same. However, if the bases do not match, the measurement results will be random.

The next step is key reconciliation, where Alice and Bob use error correction techniques to correct any discrepancies in their measurement results. This ensures that they have a consistent set of bits for the shared key. Once the key reconciliation is complete, Alice and Bob perform a key confirmation step to verify the security of the generated key. They randomly select a subset of the key bits and compare them to check for any potential eavesdropping.

If no errors or discrepancies are found during the key confirmation step, Alice and Bob can proceed to use the generated key for secure communication. However, if errors are detected, it indicates the presence of an eavesdropper, commonly referred to as Eve. The security of QKD lies in the fact that any attempt by Eve to intercept or measure the quantum states will introduce errors, which can be detected by Alice and Bob during the key reconciliation and confirmation steps.

It is important to note that QKD is a classical experiment that utilizes the principles of quantum mechanics. The physical components used in QKD, such as lasers and detectors, are classical in nature. However, the security of

the key distribution process is based on the quantum properties of the exchanged states.

Practical quantum key distribution (QKD) is a powerful tool in the field of cybersecurity that enables secure key exchange between two parties. By leveraging the principles of quantum mechanics, QKD provides a provably secure method for key distribution, making it resistant to advanced computational attacks. Understanding the fundamentals of QKD is crucial for professionals and researchers in the field of cybersecurity.

Quantum cryptography is a fascinating field that involves the use of quantum mechanics to secure communication. However, setting up a true quantum optical setup can be expensive and not easily accessible to many educational institutions. To address this, an analogy kit has been developed to enable teaching about quantum cryptography in a more affordable and practical way.

The kit has been successfully implemented in a university in Germany, where students have access to a dedicated room for performing experiments related to quantum cryptography. The feedback from students has been positive, with the kit being in high demand. This is because quantum cryptography is a topic that generates a lot of interest, but few people have a clear understanding of the actual process and the secure nature of quantum communication.

One frequently asked question is whether quantum cryptography requires polarization entanglement. While there are protocols that use polarization entanglement, the specific protocol used in the kit, known as bb-84, does not rely on it. This can be verified by looking at the publication dates of the different protocols. The bb-84 protocol was published in 1984, and polarization entanglement is not mentioned in it. Protocols involving polarization entanglement were published in later years. So, while it is possible to use entanglement, it is not a requirement for quantum cryptography.

Another common question is how quantum cryptography works in practical scenarios, considering the challenges of transmitting photons over long distances. The concern is that photons can scatter or be absorbed by the air or particles, leading to a loss of information. In practice, a technique called "decoy states" is used to overcome this challenge. Instead of sending one bit per photon, decoy states are employed to ensure practicality and increase the efficiency of the communication. Further details on this technique can be found by researching the term "decoy states."

The analogy kit for quantum cryptography provides a valuable tool for teaching the fundamentals of this exciting field. It allows learners to gain a working understanding of the quantum communication process and the secure nature of quantum cryptography. The kit does not require polarization entanglement, and practical challenges are addressed through the use of decoy states. By exploring this topic further, one can delve into the intricacies of quantum cryptography and its applications in cybersecurity.