ISSN:0975-9646

Secret Key Generation and Eavesdropping detection using Quantum Cryptography

Neha Chhabra
Asst. Prof.(CSE Deptt,) GNI, Mullana

Abstract:*Quantum Cryptography is based upon the use of quantum effects and extends those effects for conventional cryptographic methods. The two major advantages of quantum cryptography over conventional cryptography are true random secret key generation and eavesdropping detection. Quantum cryptography has been developed which promises more secure communication than any existing technique and cannot be compromised by quantum computers.*

1. INTRODUCTION

Cryptography is the art of encoding and decoding messages and has existed as long as people have distrusted each other and sought forms of secure communication. The purpose of cryptography is to transmit information such that only the intended recipient receives it. Today's most common encryption methods are threatened by the potential creation of the quantum computer.

Although work on quantum cryptography was begun by Stephen J. Wiesner in the late 1960's, the first protocol for sending a private key using quantum techniques was not published until 1984 by Bennett and Brassard.

1.1 DIFFICULTIES OF CLASSICAL CRYPTOGRAPHY:

The development of quantum cryptography was motivated by the short-comings of classical cryptographic methods. These methods are of two types: "public-key" or "secret-key" methods.

1.1.1 Public-key encryption

Public-key encryption is based on the idea of a safe with two keys: a public key to lock the safe and a private key to open it. Using this method, anyone can send a message since the public key is used to encrypt messages, but only someone with the private key can decrypt the messages. The security of public-key encryption depends on the assumed difficulty of certain mathematical operations, such as factoring extremely large prime numbers.

1.1.2 Problems in Public-key encryption

There are two problems with basing security on the assumed difficulty of mathematical problems.

1. The first problem is that the difficulty of the mathematical problems is *assumed*, not proven. All security will vanish if efficient factoring algorithms are discovered.
2. The second problem is the threat of quantum computers. The theoretical ability of quantum computers to essentially process large amounts of information in parallel would remove the time barrier to factoring large numbers.

1.1.3 Secret-key encryption

Secret-key encryption requires that two users first develop and securely share a secret key, which is a long string of randomly-chosen bits. The users then use the secret key along with public algorithms to encrypt and decrypt messages. The algorithms are very complex, and can be designed such that every bit of output is dependent on every bit of input .Suppose that a key of 128 bits is used. "Assuming that brute force, along with some parallelism, is employed, the encrypted message should be safe: a billion computers doing a billion operations per second would require a trillion years to decrypt it".

1.1.4 Problems in Secret-key encryption

There are two main problems with secret-key encryption.

1. The first problem is that by analyzing the publicly-known encrypting algorithm, it sometimes becomes easier to decrypt the message. This problem can be somewhat offset by increasing the length of the key.
2. The second problem is securely distributing the secret key in the first place. This is the well known "key-distribution problem". Users must either agree on the secret key when they are together in the same location or when they are in different locations.

2. SECURITY FEATURE OF QUANTUM CRYPTOGRAPHY

Quantum cryptography solves the problems of secret-key cryptography by providing a way for two users who are in different locations to securely establish a secret key *and* to detect if eavesdropping has occurred. In addition, since quantum cryptography does not depend on difficult mathematical problems for its security, it is not threatened by the development of quantum computers.

The security of quantum cryptography relies on the foundations of quantum mechanics, in contrast to traditional public key cryptography which relies on the computational difficulty of certain mathematical functions, and cannot provide any indication of eavesdropping or guarantee of key security. Quantum cryptography is only used to produce and distribute a key, not to transmit any message data. This key can then be used with any chosen encryption algorithm to encrypt and decrypt a message, which can then be transmitted over a standard communication channel.

Quantum cryptography accomplishes these remarkable feats by exploiting the properties of microscopic objects such as photons. Since photon polarization measurements form the foundation for the most common quantum cryptographic techniques, it is important to first understand their properties. The most important unit of information in computer science is the bit.There are two possible values that can be stored by a bit: the bit is either equal to "0" or equal to "1." These two different states can be represented in various ways, for example by a simple switch or by a capacitor: if not charged, the capacitor holds the value zero; if charged, it holds the value one. There exist many possibilities to physically represent a qubit in practice, as every Quantum system with at least two states can serve as a qubit. For example, the spin of an Atom or the polarization of a light particle can represent the state of a qubit. Even a cat with its two basic states "dead" and "alive," introduced by Schrödinger to visualize fundamental concepts of quantum mechanics, might serve as a representation.

Photons are the smallest measures of light and they can exist in all of their possible states at once, called the wave function. This means that whatever direction a photon can spin in, it does all at once. Light in this state is called unpolarized. The foundation of quantum physics is the unpredictability factor. The unpredictability is defined by Heisenberg's uncertainty principle which states that "it is impossible to know both an object's position and velocity at the same time".

But when dealing with photons for encryption, Heisenberg's principle can be used to our advantage. To create a photon, quantum cryptographers' use -- light emitting diodes, a source of unpolarized light. LEDs are capable of creating just one photon at a time, which is how a string of photons can be created, rather than a wild burst.

Through the use of polarization filters, we can force the photons to take one state i.e. to polarize it. If we use the vertical polarization filter situated beyond the LED, we can polarize the photons that emerge. The photons that are not absorbed will emerge on the other side with a vertical spin. The thing about photons is that once they're polarized, they can't be accurately measured again, except by a filter like the one that initially produced their current spin. So if a photon with a vertical spin is measured through a diagonal filter, either the photon won't pass through the filter or the filter will affect the photon's behavior, causing it to take a diagonal spin. In this sense, the information on the photon's original polarization is lost and so, too, is any information attached to the photon's spin.

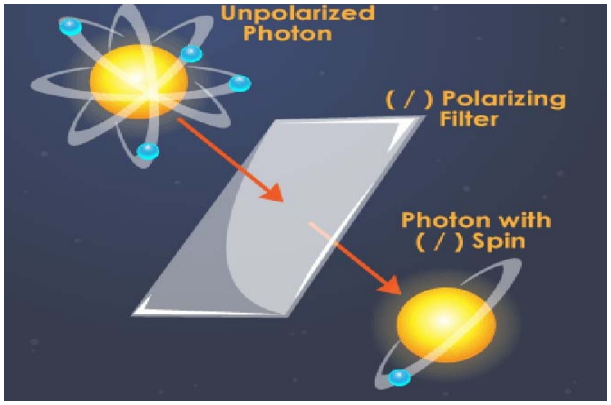

Fig.2.1 Polarization of Photons

3. UTILIZATION OF POLARIZATION EFFECTS OF PHOTONS

The three chosen bases of polarization and the possible results of a measurement according to the basis are:

a. rectilinear (horizontal or vertical),
b. circular (left-circular or right-circular), and
c. Diagonal (45° or 135°).

Although there are three bases, only two bases are used in any given protocol for quantum cryptography.

Photons can be measured to determine their orientation relative to one of these bases of polarization at a time. Classically, one would expect the photon to *have* a certain polarization, which can be measured but which is not changed by the measurement. Photons, however,

are quantum objects, and in the quantum world an object can be considered to have a property only *after* you have measured it, and the type of measurement impacts the property that you find the object to have. This implies that a photon can only be considered to *have* a particular polarization *after* you measure it, and that the basis you choose for the measurement will have an impact on the polarization that you find the photon to have. For example, if you send a photon through an apparatus to measure its orientation relative to a rectilinear coordinate system, you are asking the question, "How is the photon oriented relative to a rectilinear coordinate system?" You will find the photon is either vertically polarized or horizontally polarized -- there are only two possibilities. Suppose you measure this photon as horizontally polarized. Next you send this same photon through an apparatus to measure its orientation relative to a diagonal coordinate system. Now you are asking the question, "How is the photon oriented relative to a diagonal coordinate system?", and you will find that the photon is either 45 ° polarized or 135° polarized – there are only two possibilities.

The type of measurement does indeed have an impact on what property you find. This is in surprising contrast to the classical situation where something that is horizontally oriented would be expected to have a component in the diagonal direction. The fact that a horizontally-oriented photon may subsequently be measured to have a 45° polarization occurs because the state of horizontal polarization is actually a superposition of the two diagonal polarization states. All polarization states are actually superpositions of other polarization states.

It is important to note that once the diagonal measurement was made, all information about the previous "property" of horizontal polarization of the photon vanished. As a result it is impossible to determine a photon's rectilinear and diagonal polarizations at the same time. This is analogous to the impossibility of specifying a particle's position and momentum at the same time. More information about one results in less information about the other.

The behavior of photons sent through a series of polarizers is illustrated below:

⊕ = an apparatus that measures rectilinear polarization
↑ = vertical polarization
→ = horizontal polarization
⊗ = an apparatus that measures diagonal polarization
↗ = 45 ° polarization
↖ = 135 ° polarization

Quantum cryptography uses photons to transmit a key. Once the key is transmitted, coding and encoding using the normal secret-key method can take place. But how does a photon become a key? How do you attach information to a photon's spin? This is where binary code comes into play. Each type of a photon's spin represents one piece of information -- usually a 1 or a 0, for binary code. This code uses strings of 1s and 0s to create a coherent message. For example, 11100100110 could correspond with h-e-l-l-o. So a binary code can be assigned to each photon -- for example, a photon that has a vertical spin (↑) can be assigned a 1. Alice can send her photons through randomly chosen filters and record the polarization of each photon. She will then know what photon polarizations Bob should receive.

Figure shows how a bit can be encoded in the polarization state of a photon in BB84. We define a binary 0 as a polarization of 0 degrees in the rectilinear bases or 45 degrees in the diagonal bases. Similarly a binary 1 can be 90 degrees in the rectilinear bases or 135 in diagonal bases. Thus a bit can be represented by polarizing the photon in either one of two bases.

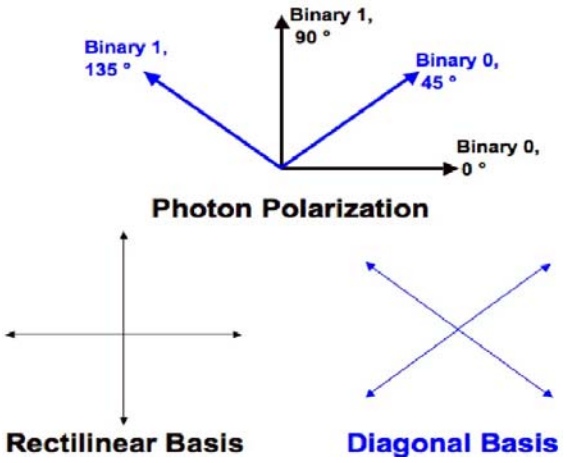

Fig 3 Basis For Polarization of Photons

4. BB84 PROTOCOL

The first quantum cryptographic protocol was introduced in 1984 by Charles H. Bennet of IBM New York and Gilles Brassard of the Universtiy of Montreal. In opposition to public key systems this protocol is based upon the generation of random secret (private) encryption and decryption keys.

4.1 Principle

First Alice transmits a random sequence of qubits over the quantum channel to Bob. She generates this sequence by repeatedly encoding a randomly selected bit value (0 or 1) into an also randomly selected base from 2 different bases. This results in yet another random sequence of 4 different quantum states, which she sends to Bob via the quantum link. Alice records the base-value-combinations she used during generation for later use.
The 2 bases are applied for encoding and also for decoding. Furthermore they must fulfill the requirement of yielding the correct result when aligned and producing an indeterministic result when they are not aligned.

4.1.1 Key Generation

When not intercepted Bob receives the Qubits directly from Alice. Since Alice transmitted only the Qubits without any further information, the only way for Bob to derive any information from the incoming qubit is to measure them against a randomly selected sequence of bases of his own. If he selects the same base, which was used for encoding, then the result is determined to be correct. When the bases are different, then the result of this measurement is indeterministic. Bob records both his own sequence of bases and the results he measured.
After that Alice and Bob communicate via conventional means to compare their sequences of applied bases. They keep only those values, where both used the same base for encoding and decoding. The other bits are discarded from the sequence of values. This remaining sequence is a purely random private raw key and is called the sifted key. Since this raw key may not be suitable for encryption and decryption it can still be used as seed to generate such a key as long as Alice and Bob apply the same cryptographic algorithms.

The actual encryption, transmission and decryption of content is performed by conventional means over standard communication lines as long as secret key protocols are implemented. Optimum privacy can be achieved by generating an encryption key, which is as long as the document to be secured. This way, every single byte of data can be encrypted with its own randomly generated byte of the whole key. Such encrypted data contains no patterns of itself anymore, which could otherwise be used as basis for attempts of code breaking.

4.1.2 Eavesdropping Detection

When Eve listens on the quantum channel she intercepts the qubits sent by Alice and performs her observations before resending her results to Bob. Since Eve has to follow same physical laws as Bob does the only way for Eve to get any information out of the qubits sent by Alice is to apply her own sequence of bases when measuring them. The results obtained by Eve also obey the rules of determinism and indeterminism when being measured. Thus all the bits measured by Eve with a different base than Alice have a maximum probability of 50 % of being wrong.

4.2 Single Photon Polarization

The 4 bases and value states are encoded in the polarization angles of single photons as In:

Table 4.1 Basis & Value Encoding

Basis	Value	Angle	Polarization
⊕	0	0	→
⊕	1	90	↑
⊗	0	45	↗
⊗	1	135	↖

5. PROPOSED WORK

5.1 Qubit Combinations

The following table shows the possible qubit combinations which can occur in an error free and undisturbed quantum channel.

	combination	01	02	03	04	05	06	07	08	09	10	11	12
Alice	basis	⊕	⊕	⊕	⊕	⊕	⊕	⊗	⊗	⊗	⊗	⊗	⊗
	value	0	0	0	1	1	1	0	0	0	1	1	1
	polarization	→	→	→	↑	↑	↑	↗	↗	↗	↖	↖	↖
Bob	basis	⊕	⊗	⊗	⊕	⊗	⊗	⊗	⊕	⊕	⊗	⊕	⊕
	polarization	→	↗	↖	↑	↗	↖	↗	→	↑	↖	→	↑
	value	0	0	1	1	0	1	0	0	1	1	0	1
	correct	✓	✓	x	✓	x	✓	✓	✓	x	✓	x	✓

Fig 5.1 Qubit combinations

The combinations 1, 4, 7 and 10 use the same basis for encoding and decoding, so the value sent by Alice yields the same value measured by Bob. These bits will be used as raw key material. All other combinations use different bases and thus have a 50 % probability of yielding either the same (2, 5, 8, and 11) or the other (3,

6, 9 and 12) value. The bits acquired through these combinations will not be used for key generation.

5.2 Key Generation

The first and main objective of quantum cryptography is to generate true random secret raw key material. This is performed by the following steps.

5.2.1 Alice sends Random Qubit Sequence

Alice encodes her part of the key with a random sequence of bases and by this generates a random sequence of qubits, which is transmitted over the quantum channel.

basis	⊕	⊕	⊗	⊗	⊕	⊕	⊕	⊕	⊗	⊗	⊗	⊗
value	0	1	0	1	0	0	1	1	0	0	1	1
polarization	→	↑	↗	↖	→	→	↑	↑	↗	↗	↖	↖

Fig 5.2 Bits sent by Alice

5.2.2 Bob measures incoming Qubits

Bob measures the incoming qubits against his own random sequence of bases and records the received values. If Bob selected the same base as Alice then he will measure exactly the same value, which was originally encoded by Alice. Otherwise the polarization of the incoming photon is unaligned with equal distance to the 2 possible polarizations of the applied base.

basis	⊕	⊕	⊗	⊗	⊗	⊗	⊗	⊗	⊕	⊕	⊕	⊕
polarization	→	↑	↗	↖	↗	↖	↗	↖	→	↑	→	↑
value	0	1	0	1	0	1	0	1	0	1	0	1

Fig 5.3 Bits measured by Bob

5.2.3 Alice and Bob compare Bases

Alice and Bob compare the sequences of their applied bases. The bits which were sent and received using the same base yield the same value and can be used as raw key material. On the other side there are the bits, where they used different bases, which are discarded, because they have a 50 % chance of being wrong. The following Table shows, that whenever the bases are aligned the result is correct.

aligned	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗
correct	✓	✓	✓	✓	✓	✗	✗	✓	✓	✗	✗	✓
sifted key	0	1	0	1								

Fig 5.4 Sifted key

5.2.4 Alice and Bob generate True Random Secret Key

Since Alice and Bob select random sequences of bases independently of each other the resulting sequence of corresponding bases is purely random. Due to the indeterminism of qubits measured with unaligned bases Eve has no indication whether her values are right or wrong.

5.3 Eavesdropping Detection

The Goal of Eve is to obtain the actual content, which is transmitted without being detected doing so. To achieve this she applies an intercept and resend technique on both the conventional and the quantum channel. This means she listens on the communication channels and intercepts any signals sent by Alice. Then she may try to perform copy or read operations before she resends the signal to Bob. However, in quantum cryptography all these actions by Eve result in permanent quantum effects on the transmitted signals.

5.3.1 Alice sends Random Qubit Sequence

Alice generates her random qubit seqence and transmits it via the quantum channel to Bob in the same way, whether this transmission is being listened upon or not.

basis	⊕	⊕	⊗	⊗	⊕	⊕	⊕	⊕	⊗	⊗	⊗	⊗
value	0	1	0	1	0	0	1	1	0	0	1	1
polarization	→	↑	↗	↖	→	→	↑	↑	↗	↗	↖	↖

Fig 5.5 Bits sent by Alice

5.3.2 Eve performs intercept & resend eavesdropping

Eve now intercepts the photons from Alice and may perform the following actions. When cloning the photon the no cloning theorem inhibits the clone from being an exact copy of the original state. Thus at least one photon is modified by the process and will cause errors, whether it is resent to Bob or kept by Eve. If Eve decides to perform her measurements on the original photon before resending it to Bob the following situation occurs. By measuring the polarization of a photon the particle adopts exactly the same polarization which was measured. This is asserted by the 5th axiom of quantum theory which causes every measurement to have an effect on the measured object. Thus again the photon resent to Bob will cause detectable errors. Even worse for Eve her measurements also follow the same indeterminism that holds for Bob.

basis	⊕	⊕	⊗	⊗	⊗	⊗	⊗	⊗	⊕	⊕	⊕	⊕
polarization	→	↑	↗	↖	↗	↖	↗	↖	→	↑	→	↑
value	0	1	0	1	0	1	0	1	0	1	0	1

Fig 5.6 Bits measured by Eve and resent to Bob

5.3.3 Bob measures incoming Qubits

Bob also receives and measures the incoming qubits in the same manner, regardless of possible eavesdropping by Eve. Even though the eavesdropping attempts by Eve caused an error rate of approximately 25 % this is not yet obvious to Bob. This time the alignment between Eve's and Bob's bases decide over determinism or indeterminism.

basis	⊕	⊕	⊗	⊗	⊕	⊗	⊕	⊗	⊗	⊗	⊗	⊗
polarization	→	↑	↗	↖	→	↖	↑	↗	↗	↖	↖	↗
value	0	1	0	1	0	1	1	0	0	1	1	0

Fig 5.7 Bits measured by Bob

5.3.4 Alice and Bob compare Bases

This part of the protocol also performs in exactly the same way, as if not intercepted. Eve may listen on the conventional channel and obtain all the information shared by Alice and Bob, which is transmitted over this line. Thus Eve can also compare her own random sequence of bases with both the sequences of Alice and Bob. This also reveals to Eve, which of her measurements yielded the right result. The privacy is kept by the fact that Alice and Bob perform a different pattern matching than Eve and thus obtain a secret key, which is not known to Eve. In the following table it is shown that in this case situations exist, where Alice and Bob have aligned bases but Bob's values are not correct.

aligned	✓	✓	✓	✓	✓	✘	✓	✘	✓	✓	✓	✓
correct	✓	✓	✓	✓	✓	✘	✓	✘	✓	✘	✓	✘
sifted key	0	1	0	1	0		1		0		1	

Fig 5.8 Sifted but intercepted key

5.3.5 Alice and Bob compare Sample of Values

To maintain security Alice and Bob will also compare small portions of their keys. The interception by Eve shifted the polarization of those photons, which were measured by her using a different base than Alice. These shifted photons cause the result of Bob's measurement to be indeterminate even if his base is aligned with Alice's base. When performing error correction according to standard methods, Alice and Bob will detect an above average error rate.

5.3.6 Alice and Bob detect Eavesdropping

After Alice and Bob detected the eavesdropping attempt by Eve they can discard the whole raw key and postpone their communication to a point when they are not listened upon any more. If this is not an option they still have the opportunity to amplify their privacy by discarding only those bits, which were communicated for error correction. The remaining sifted key can then be further modified to decrease the ratio of information available to Eve. Again all bit values revealed over the conventional must not be included in the final key. This way Alice and Bob receive a shortened but truly secret key.

6. PRACTICAL APPROACH

The practicalities of performing transmissions on a quantum channel are not as simple as the theory. The light source is usually an LED or laser, and the sender produces a low-intensity polarized beam that is emitted in short bursts. The polarization of each burst is randomly modulated to either horizontal, vertical, left-circular, or right-circular before being sent on to the receiver. Recently, researchers at the University of

California at Santa Barbara have reported that they have found a way to emit single photons. Single photon emission would prevent Eve from skimming off part of a photon burst, making it possible to produce a key that is "secure from the most advanced attacks."

The quantum information in the form of polarized photons may then be sent over optical fiber or through free space, also called free space optics (FSO).The difficulty with sending quantum information over optical fiber is that polarizations are not retained over long distances. Improvements in optical fiber may help extend the distance over which such information can be sent. Another possible way to extend the distances is to use interferometry, looking at differences in phase instead of polarization. Using fiber optic cables, photon bits have successfully been transmitted over distances up to 60 km, which is about 37 miles. Transmitting through the air eliminates the problems of impurities in optical fiber, but so far, successful transmission has been over shorter distances and the weather conditions must be ideal. In early 2002, researchers exchanged a key at night from the mountaintops at Zugspitze and Karwendelspitze in Germany. This transmission over 23.4 km was a record. Los Alamos National laboratory has reported an exchange over 1.6 km during daylight. Such transmissions could be useful in military applications, where the key is exchanged from one ground station to a satellite and then to another ground station.

7.CONCLUSION AND FUTURE SCOPE

Whether quantum cryptography will replace classical cryptography techniques will depend on many factors including transmission distance, expense, and ease of use. It is suspected that quantum cryptography is already being used between the White House and the Pentagon .There may also be connections between certain military cites, large defense contractors, and research laboratories that are not very far apart. A possible commercial application that could utilize quantum cryptography is "two-party secure computation" in which two parties compare results of a computation without revealing the data used by each party to complete the computation. Since the two parties could be sitting at the same table, distance is not a problem.

Quantum Cryptography can be performed independently of the availability of quantum computers since the qubits are only transmitted and received, without performing any quantum operations on single qubits or even sequences of qubits (quantum registers). Communication via the quantum channel is only required during the phase of key generation to provide the desired privacy for key exchange. The actual transmission of encrypted data occurs on conventional communication lines and application of conventional secret key cryptographic methods.

Quantum cryptography promises to revolutionize secure communication by providing security based on the fundamental laws of physics, instead of the current state of mathematical algorithms or computing technology. The devices for implementing such methods exist and the performance of demonstration systems is being continuously improved. Within the next few years, if not months, such systems could start encrypting some of the most valuable secrets of government and industry. Future developments will focus on faster photon detectors, a major factor limiting the development of practical systems for widespread commercial use. Chip Elliott, BBN's principal engineer, says the company is working with the University of Rochester and NIST's Boulder Laboratories in Colorado to develop practical superconducting photon detectors based on niobium nitride, which would operate at 4 K and 10 GHz. The ultimate goal is to make QKD more reliable, integrate it with today's telecommunications infrastructure, and increase the transmission distance and rate of key generation. Thus the Long-term goals of quantum key distribution are the realistic implementation via fibers, for example, for different buildings of a bank or company, and free space key exchange via satellites. Quantum cryptography already provides the most advanced technology of quantum information science, and is on the way to achieve the (quantum) jump from university laboratories to the real world.

8. References

1. Quantum Cryptography: A Survey ACM Computing Surveys, Vol. 39, No.2, Article 6, Publication date: June 2007
2. http://en.wikipedia.org/wiki/Quantum_cryptography
3. http://www.aip.org/tip/INPHFA/vol-10/iss-6/p22.html
4. http://www.perimeterinstitute.ca/personal/dgottesman/QKD.html
5. http://www.cs.brandeis.edu/pablo/qbc/node4.htm

AUTHORS PROFILE

Neha Chhabra received the bachelor degree in Computer Science and Engineering from Haryana Engineering College, Jagadhri, India in 2010.Currently persuing Masters in CSE From Kurukshetra University. She has 2 year teaching experience. Presently she is working in Computer Science and Engineering Department of Guru Nanak Institutions Mullana.