Performance Analysis for Secret Message Sharing using Different Levels of Encoding Over QSDC

Nur Shahirah Binti Azahari[1], Nur Ziadah Binti Harun[2], Chai Wen Chuah[3],
Rosmamalmi Mat Nawi[4], Zuriati Binti Ahmad Zukarnain[5], Nor Iryani Binti Yahya[6]
Faculty of Computer Science and Information Technology, University Tun Hussein Onn Malaysia,
86400 Parit Raja, Johor, Malaysia[1, 2, 4]
Guangdong University of Science and Technology[3]
Faculty of Computer Science and Information Technology, University Putra Malaysia, 43400 Serdang, Selangor[5]
Kita Ryo Trading, 177A Jalan Kenanga 29/4, Taman Indahpura 81000, Kulai, Johor, Malaysia[6]

***Abstract*—It was recently proposed to use quantum secure direct communication (QSDC), a branch of quantum cryptography, to secure data transfers from sender to receiver without relying on computational complexity. Despite the benefits of multiphoton, sending secret messages between several parties in a quantum channel still presents a challenge because the current multiphoton only considers two parties. When more parties are included, the scalability problem becomes apparent. Therefore, the scalable multiphoton approach is needed to allow secure sharing between the legal parties. The manipulation of level encoding provides new opportunities for more efficient quantum information processing and message sharing. This research aims to propose a strategy that uses four-level encoding with the multiphoton approach to share secret messages between multi-party. From the analysis conducted, it has been shown that a high number of level encoding can shorten the time taken for photon transmission between parties and an attacker has a lower probability of chances to launch an attack, however, communication will be affected due to high sensitivity to noise.**

***Keywords*—Multiphoton approach; multi-party; level of encoding; scalability; error probability**

I. Introduction

Quantum secure direct communication (QSDC) is derived from the quantum communication channel and can transfer secret messages without the use of a private key [1]. These are further supported by studies done by [2], [3], which found that no secret key is needed to transport a secret sharing message in QSDC. The fundamental principle of secret sharing is that the secret holder splits a section of complete secret information into many parts and distributes all of them to various participants for keeping [4]. A single individual can't acquire adequate secrets. Complete secret information can only be discovered when everyone cooperates. Decentralized handling of secret information is achieved by secret sharing, which also contributes to minimizing eavesdropping risks while embracing some attacks and mistakes [5]. Furthermore, major applications of the secret sharing protocol include key agreement, secure multi-party computing, and voting systems [6], [7]. In other words, secret message sharing is a method for dividing and distributing a secret message across numerous parties, whereas QSDC provides direct secure communication without a shared secret key. While both QSDC and secret message sharing provide distinct functions in certain circumstances, they can be combined to achieve secure and efficient cryptographic processes.

In the QC field, a single photon transmission per laser pulse is the most fundamental technique. It is challenging to produce one photon per laser pulse. In the worst case, less than one photon will be produced in each time slot by the weak optical beam, and the slots will be mostly empty [8]. Many empty pulses will lower the transmission rate. It is only suitable for short-range communication since it is challenging to make sure that a single transmission photon stays stable throughout a long-distance channel [9]. This is the result of errors like channel loss and network disruption due to eavesdroppers. Due to their poor performance across long distances and their low data rates, single photons are also vulnerable to PNS attacks since they can unintentionally emit more than one photon per time slot. One advantage that multiphotons have over single photons is that they have faster transmission rates and longer photon travel distances [10]. In the multiphoton technique, information exchange is not limited to the presence of a single photon in a time slot. Multiphoton is analogous to sending the same message many times. Any unitary transformation will have the same effect on the photons regardless of how many photons the laser pulse generates as long as they are all in the same phase [10]. Despite the benefits of multiphoton, sending secret messages between several parties in a quantum channel still presents a challenge because the current multiphoton considers two parties. When more parties are included in the quantum network, the scalability problem becomes apparent.

Levels of encoding have attracted attention recently because of their potential use in several branches of quantum information technology, including quantum computing, quantum communication, and quantum cryptography. It is feasible to encode and process more information, as well as carry out more difficult quantum processes, in systems with more dimensions. A qudit, which is a generalization of a qubit to a system with d levels of encoding, is one illustration of a high-dimensional quantum state [11]. A qudit can have more dimensions than a qubit, whereas a qubit is a 2-dimensional quantum state ($d = 2$). The high number of level encoding can differ significantly from qubits in terms of their features and behavior, opening up new possibilities for quantum information processing. Using a high number of level encoding has several benefits. A high number of level encodings have

been found to be more resistant to quantum cloning than qubit operations [12].

In this paper, the HMBSS [13] protocol is considered as the main benchmark for the proposed message sharing among multi-party. HMBSS protocol implemented a multiphoton approach for sharing secret messages but only two-party participants. The existing multiphoton approach could not share information between more than two parties. Therefore, the scalable multiphoton approach is needed to allow multiple secure sharing between the legal parties with the idea of integrating a high dimensional quantum state.

The remaining content of the paper is formatted as follows: Section II, a synopsis of related works. In Section II, a potential approach is analyzed. In Section IV, the simulation setup is examined. Evaluation of performance is covered in Section V. The result and conclusion are covered in Section VI. Finally, Section VII discusses the conclusions.

II. Related Work

QSDC is a sort of quantum communication that transfers data securely through a quantum channel. The multiphoton approach is more sophisticated and offers benefits including high transmission rates and long photon travel distances compared to single photon [10]. The same quantum state can be transferred several times due to information sharing in a multiphoton approach. To increase the chance that the transmission will be successful, a multiphoton can be sent at once to represent a single bit of information.

In 2019, a Hybrid Mary in Braided Single Stage (HMBSS) with a multiphoton approach has been proposed [13]. This protocol uses a compression strategy and a lossless data encoding foundation to reduce the amount of photons needed during the data transmission phase. In 2017, A. Sit *et al* proposed high-dimensional intracity quantum cryptography with structured photons [14]. The protocol encodes information using a single photon. The protocol has demonstrated that, despite a noisy channel, it is possible to increase the secure data transmission rate utilizing high-dimensional quantum states as compared to bidimensional states. In 2018, Y. Jo *et al.* proposed efficient high dimensional with hybrid encoding [15]. Efficient Information Reconciliation for High-Dimensional has been proposed by R. Mueller *et al.* in 2023. Both protocols demonstrate that the proposed viable approach has significantly improved the secret key rate over the 2-dimensional protocol. M. De Oliveira *et al.* conducted an experiment on high-dimensional with spin-orbit-structured photons in 2020, demonstrating a protocol that is easily scalable in both dimensions and enables information sharing between participants [16]. In 2023, C. Sekga et al. proposed a high-dimensional implementation with biphotons [17]. Information is encoded using biphotons in this protocol, and the biphotons are used as qutrits to increase error tolerance. A higher number of levels used for encoding provides high efficiency [16], [18], [19]. The efficiency of communication can be measured by mutual information between the parties involved. The mutual information between parties in quantum communication is an indicator of the shared information between their quantum states. From fidelity, mutual information between parties involved can be calculated. As a result, increasing the dimensionality of protocols certainly has an increased capacity for mutual information [18].

Nonetheless, a few protocols from the mentioned protocol above are just for one-to-one communication. Hence, they do not achieve scalability in terms of the number of parties involved in communication. Therefore, a scalable multiphoton approach is required to enable secure sharing between the legal parties. Other than that, the protocol that implemented a 2-level encoding that will detect the sequence of photons as “00”, “01”, “10” and “11”, will result in a low transmission rate. A low transmission key happens because a lot of photons are lost during the transmission [20]. Next, this protocol also implemented a single photon. Single photons have its limitations [8]. The number of photons that can pass through the quantum channel will be restricted by the laser source's single photon output per pulse. Additionally, it is quite difficult to create one photon for every laser pulse. Less than one photon will be produced by the weak optical beam for each time slot, and the worst-case scenario is that most of the time the slots are empty [8]. A high amount of empty pulses results in a low transmission rate.

All in all, the protocols mentioned have their drawbacks. This paper suggests a Quantum Multiparty 4-level encoding Secret Message Sharing protocol (QM4SMS) with multiphoton to address the aforementioned issues. In this protocol, we provide a 4-level encoding schematic setup with a multiphoton approach to share a secret message between multiple parties over QSDC. We show that different numbers of levels used for encoding, where d is 2, 3, or 4 can fasten the photon transmission. Note that in this paper, d denotes the levels encoding or quantum state's dimension. We also analyzed the total time taken to transmit photons with different levels of d. Table I shows the comparison between the mentioned protocols.

TABLE I. Comparison among some Different Level Encoding

Protocol	d	Multiparty	Photons Source	Benefit	Limitation	Performance Metric
HMBSS [13]	2	No	Multiphoton	Utilize the Huffman compression technique to reduce memory usage and increase transmission rates by lowering transmission time while retaining message confidentiality.	No authentication procedure is used while exchanging information to guarantee that the message is kept private between parties.	• Total transmission time to encode photons. • Compression ratio.
Intracity quantum cryptography with structured photons [14]	4	No	Single photon	Extendable over greater distances.	The absence of active wavefront correction and moderate turbulence.	• Secret Key Rate (SKR)

						• Quantum Bit Error Rate (QBER)
Efficient Hybrid Encoding [15]	2,3,4,5	No	Single photon	Protection from side channel assaults against detectors and practicality of the experiment.	Less reliable than measuring device-independent (MDI).	• SKR • Transmission Loss • QBER
Spin-orbit-structured photon [16]	2 & 3	Yes	single photon	High fidelity.	The inaccuracies are caused by additional flaws in the half waveplates, which cause a minor misalignment in the setup and use of a weak coherent photon source.	• Fidelity • Mutual Information • QBER
Efficient Information Reconciliation [21]	4 & 8	No	Single photon	Allows reconciliation with high efficiency and minimal interaction.	With higher error rates, the time required for executing the correction increases significantly.	• SKR • QBER
DIQKD [17]	3	No	Biphoton	Utilized the biphotons as a qutrit to increase the error rate tolerance.	Bell experiments without holes are necessary, making it impossible to realize using current technologies.	• SKR • QBER

III. Proposed Protocol

This paper suggests Quantum Multiparty 4-level encoding Secret Message Sharing protocol (QM4SMS) with multiphoton. In the proposed protocol, 2-*d*, 3-*d* and 4-*d* level encoding signals have been implemented with the Huffman encoding. The proposed protocol will employ Huffman encoding to compress the message's source at the sender [13]. The benefit of employing Huffman encoding because it is a lossless compression technique used to send unreadable messages more securely and effectively. Lossless refers to the ability to precisely retrieve the original message from a compressed message stream. QM4SMS will shorten the number of bits and encode it in an unknown format. The Huffman decompression algorithm will be used at the receiver to decode the compressed messages. The Huffman encoding procedure is straightforward. Where the Huffman compression method is used by the sender to protect the confidentiality of the transmitted message. In this study, the message is encoded using the ASCII coding system as bits of 1 or 0. By mapping a certain polarisation angle to the list of bits, encryption is accomplished.

This protocol will take into account how multiparty quantum communication will be implemented. The context of multiparty in the proposed protocol is the number of parties involved in communication, and each of the parties has the same task during the communication. Some of the current protocol counts the third party as multiparty [15]–[17], [21]. Various issues will arise when third a party also known as Trent participates in communications. To fully benefit from multiparty encrypted communication, it is essential to ensure information equalization among the parties. The third party could be considered an eavesdropper. If one of the parties illegally works with the third party, there will be an information imbalance between the parties. It is crucial to rule out the possibility of information imbalance since information equity in multiparty cryptographic communication is so important.

The message is transformed directly into the input quantum state by combining a classic encoder with a quantum encoder. Alice encoder transforms the input signal to the input quantum state, photon *X*. The quantum system then receives the photon *X* and transmits it. The detector will transform the output quantum state at Bob and Charlie as a result.

Fig. 1 illustrates the QM4SMS approach's protocol. To decrease source redundancy, Alice first compresses the message with the Huffman encoding. Alice then used photon polarisation to encrypt the message's bits as 4 bits as we use 4-*d*. This paper suggests 4-*d* because it is the most stable in terms of distance and considerable error rate [15]. An authentication mechanism is required in the initial step to verify Alice, Bob, and Charlie's communication. The Huffman decoding algorithm was then used by Bob and Charlie, the receiver, to decompress and retrieve the original delivered message. Table II shows the angle of encoding that mapped to the bit representation for 4-*d*.

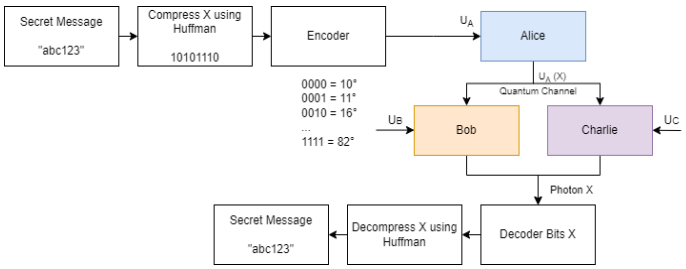

Fig. 1. QM4SMS protocol.

A. Simulation Setup

The proposed QM4SMS implementations were tested using a Python-based simulation. Python was used because it can represent quantum states mathematically. The proposed QM4SMS was evaluated in comparison to *d*-level encoding. The comparable multi-level encoding was reimplemented to achieve objectivity.

In order for the protocols to function under a similar simulator, this method is carried out using the Python

programming language. The QM4SMS protocol was then tested and validated using the same setting of the comparable level encoding, *d* to show that the suggested approach works as intended. The tested bit size for the comparing multiphoton approaches was 10. For each of the analyzed protocols, the time to convey a small amount of information and the time it takes the half-wave plate to rotate from its initial position to its new position is taken from previous studies [22]. Every eight bits, the half wave plate's update angle or rotation is changed for authentication purposes. The level of security has been enhanced at each stage due to the rapid polarization changes, although it takes longer to send the information. The simulation parameters for this experiment setting are shown in Table III.

TABLE II. ANGLE OF ENCODING AND BIT PRESENTATION

Angle of Encoding, θ	Bits Presentation
10º	0000
11º	0001
16º	0010
21º	0011
26º	0100
31º	0101
37º	0110
41º	0111
46º	1000
51º	1001
56º	1010
61º	1011
66º	1100
71º	1101
76º	1110
82º	1111

TABLE III. SIMULATION PARAMETER [13]

Parameters	Values
Bit size	10
d	2,3, and 4
Half-wave plate rotation	20.7 sec
Time to send a bit of information	4.5 sec

Three steps are involved in the suggested approach which are the encoding, transformation and decoding stages. The suggested protocol has been discussed in detail based on an experiment conducted by Azahari *et al.* [22]:

1) Encoding stage: Alice will use Huffman encoding to compress the message. According to the order of the bits, the polarising filter will encode the list of bits, described by a Mueller matrix [23].

$$M_{pol} = \frac{1}{2}\begin{bmatrix} 1 & \cos(2\theta) & \sin(2\theta) & 0 \\ \cos(2\theta) & \cos^2(2\theta) & \cos(2\theta)\sin(2\theta) & 0 \\ \sin(2\theta) & \cos(2\theta)\sin(2\theta) & \sin^2(2\theta) & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad (1)$$

The rotation of the polarizer is polarized using Eq. (1) with the angles of the polarizer as shown in Table II.

2) Transformation stage: The photons that are polarized with the angles of the polarizer as shown in Table II are then passed through HWP using Eq. (2). The HWP operation's rotation is shown as [24]:

$$M_{HWP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos(4\theta) & \sin(4\theta) & 0 \\ 0 & \sin(4\theta) & -\cos(4\theta) & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \quad (2)$$

Following is an explanation of the photon transmission process:

The protocol is used to share the $\theta_{initial}$.

Alice generates her transformation using Eq. (3) [13],

$$U_A = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & cos(4\theta_{initial}) & sin(4\theta_{initial}) & 0 \\ 0 & sin(4\theta_{initial}) & -cos(4\theta_{initial}) & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \quad (3)$$

The bits are transmitted by Alice using her transformation. Every 8 bits, the polarisation angles changed to generate θ_{next}.

3) Decoding stage: The bits of information that Alice transmitted are retrieved by Bob and Charlie by applying U_A^T to the photon they have just received. The output beam's intensity will subsequently be used by the polarizer to detect the polarisation states. Eq. (4) provides the Malus' law, which allows for the calculation of the intensity's output as describe by [25]–[27],

$$I_O = I_I \cos^2(\theta) \quad (4)$$

where, I_O is the output intensity I_I, is the input intensity and θ is the encoding or polarization angle for the specific bits. The Malus law is calculated from the top row of polarizers in Eq. (1), which is given by [13],

$$S = \frac{1}{2} \times [1 \ cos(2\theta) \ sin(\theta) \ 0] \times = \frac{1}{2} \times [1 + cos(2\theta)] \quad (5)$$

where, *S* is the input bit, Eq. (5) condensed form is obtained as [13]:

$$\frac{1 + cos(2\theta)}{2} = cos^2 \theta \quad (6)$$

To analyze the amount of time required to encode the information, a multilevel signal encoding technique was carefully developed and put into use [28], [29]. This protocol uses a signal encoding approach that enables the transmission of many bits of information simultaneously. When numerous bits are conveyed simultaneously, the channel bandwidth can be used efficiently. It has been demonstrated that higher levels

of encoding carry more data bits in each transaction. A quantitative measure of the larger information capacity is given by the relation $log_2(m)$ [30] , which returns the number of classical bits needed to encode the same amount of information [7], [31]. As illustrated in Table IV, the degree of signal encoding can be represented as up to $log_2(m)$ bits of information per symbol.

The intensity ranges are utilized to map the output into its bit representation. These intensity ranges are split up such that there is an equal probability of detecting each of all levels [29]. As a result, the angles are selected so that the output will be in the middle of each value range. The increases in dimension or level encoding, the less probability for Eve to launch an attack. Table IV shows the level of encoding and its state representation. In a 4-level encoding, each state corresponds to 2 bits of data. Each state in an 8-level encoding corresponds to three bits of data. Each state in a 16-level encoding corresponds to 4 bits of data. The advantage of multi-level encoding is that it increases the rate of data and channel efficiency by allowing each pulse to carry many bits of information.

Table V and Fig. 2 show that four polarizer state representations, denoted by the numbers 00, 01, 10 and 11, were produced via the 2-*d*. Value 00 of the polarizer state representation corresponds to a 20° encoding angle, value 01 to a 38° encoding angle, value 10 to a 52° encoding angle and value 11 to a 70°. In 2-*d*, each angle has $\frac{1}{4}$ probability for Eve to launch an attack.

Table VI and Fig. 3 show that eight polarizer state representations, denoted by the numbers 000, 001, 010, 011, 100, 101, 110, and 111, were produced via the 3-*d*. Value 000 of the polarizer state representation corresponds to a 12° encoding angle, value 001 to a 23° encoding angle, value 010 to a 34° encoding angle, value 011 to a 45° encoding angle, and value 100 to a 56° encoding angle, value 101 to a 67° encoding angle, value 110 to a 78° encoding angle, and value 111 to an 89° encoding angle. In 3-*d*, each angle has $\frac{1}{8}$ probability for Eve to launch an attack.

TABLE IV. LEVEL OF ENCODING AND STATE PRESENTATION

Level encoding (*m*)	$log_2(m)$	*d*	Bit representation
4-level	$log_2(4) = 2$	2	(00,01,10,11)
8-level	$log_2(8) = 3$	3	(000,001,010,011,100,101, 110,111)
16-level	$log_2(16) = 4$	4	(0000, 0001, 0010, 0011, 0100, 0101, 0110, 0111, 1000, 1001, 1010, 1011, 1100, 1101, 1110, 1111)

TABLE V. OUTPUT INTENSITY FOR 2-*D*

Angle of Encoding, Θ	Intensity, *I*	Bit Presentation
20	0.88302	00
38	0.62096	01
52	0.37903	11
70	0.11697	10

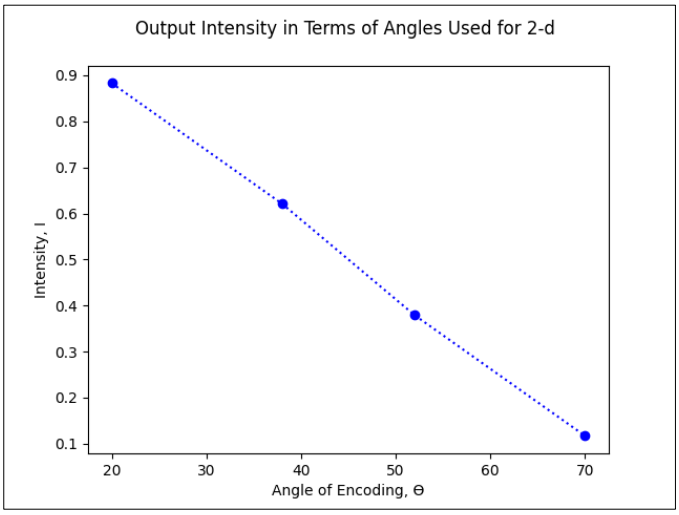

Fig. 2. Output intensity in terms of angles used for 2-d.

TABLE VI. OUTPUT INTENSITY FOR 3-*D*

Angle of Encoding, Θ	Intensity, *I*	Bit Presentation
12	0.95677	000
23	0.84732	001
34	0.68730	010
45	0.50000	011
56	0.31269	100
67	0.15267	101
78	0.04322	110
89	0.00030	111

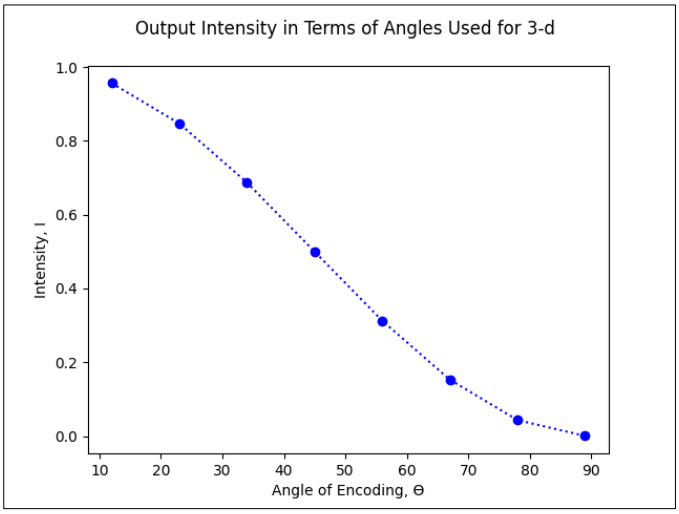

Fig. 3. Output Intensity in Terms of Angles used for 3-d.

The light beam will be received by the HWP at Bob and Charlie, and then the detector will identify the photon sequence as shown in Table VII and Fig. 4. In 4-*d*, each angle has $\frac{1}{16}$ probability for Eve to launch an attack. After receiving all the message bits, Bob and Charlie will use Huffman decoding to decode the compressed bits. The application of transformations

must be commutative, which means that only the parties applying them are aware of their existence. In this case, the only setup that has been considered is the HWP of Alice, $M_{HWP}\ (A_\theta)$. To perform the encryption, Alice will first apply her HWP, and then to reverse the effects of the initial transformation, she will use a similar rotational angle of HWP. The commutative transformation may prove demonstrated as [13]:

$$M_{HWP}\ (A_\theta).M_{HWP}\ (A_\theta)\ =\ I \tag{7}$$

where, I is the identity matrix,

$$I = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{8}$$

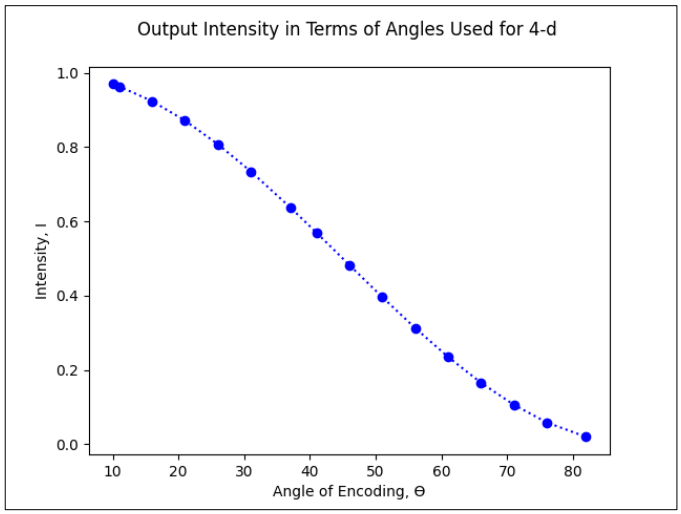

Fig. 4. Output intensity in terms of angles used for 4-d.

TABLE VII. OUTPUT INTENSITY FOR 4-D

Angle of Encoding, θ	Intensity, I	Bits Presentation
10	0.96984	0000
11	0.96359	0001
16	0.92402	0010
21	0.87157	0011
26	0.80783	0100
31	0.73473	0101
37	0.63781	0110
41	0.56958	0111
46	0.48255	1000
51	0.39604	1001
56	0.31269	1010
61	0.23504	1011
66	0.16543	1100
71	0.10599	1101
76	0.05852	1110
82	0.01936	1111

Algorithm 1 details the pseudo-code of the proposed QM4SMS approach.

Algorithm 1: QM4SMS Approach

Notation:
Transmission Time = Ø
theta ← HWP's rotation angle
time_taken ← Period of the photon transfer

Initialization:
X = (0, 1) random string message with the given bit size = 10
Alice compresses bit sequence X using Huffman:
F ← Huffman tree
B ← Bit sequence B
EncodeHuffman(F, X) ← Huffman **function** to encode the String X

Encoding stage: After passing through a linear polarizer, a photon produced represents a qubit:
pol()←is the polarization of linear polarizer using Eq. (1)
B ← pol()
for bit in B
if bit == 0000 **then**
pol_angle = 10◦
elif bit ==0001 **then**
pol_angle = 11◦
elif bit ==0010 **then**
pol_angle = 16◦
elif bit ==0011 **then**
pol_angle = 21◦
elif bit ==0100 **then**
pol_angle = 26◦
elif bit ==0101 **then**
pol_angle = 31◦
elif bit ==0110 **then**
pol_angle = 37◦
elif bit ==0111 **then**
pol_angle = 41◦
elif bit == 1000 **then**
pol_angle = 46◦
elif bit ==1001 **then**
pol_angle = 51◦
elif bit ==1010 **then**
pol_angle = 56◦
elif bit ==1011 **then**
pol_angle = 61◦
elif bit ==1100 **then**
pol_angle = 66◦
elif bit ==1101 **then**
pol_angle = 71◦
elif bit ==1110 **then**
pol_angle = 76◦
else bit ==1111 **then**
pol_angle = 82◦
end if
end for
Photon distribution:
for each (theta, time_taken) in f(B, theta, time_taken):
for j in range(len(B)):
Transmission of photon

```
if i * len(B) + j >= len(B):
break transmission
end if
end for
Decoding stage: The polarizer will next use Eq. (4) to determine the polarisation states based on the intensity level:
for each bit in B
B ← pol()
switch intensity_value
case 0.96984 then
bit == 0000
case 0.96359 then
bit ==0001
case 0.92402 then
bit ==0010
case 0.87157then
bit ==0011
case 0.80783 then
bit ==0100
case 0.73473 then
bit == 0101
case 0.63781 then
bit ==0110
case 0.56958 then
bit == 0111
case 0.48255 then
bit ==1000
case 0.39604 then
bit ==1001
case 0.31269 then
bit == 1010
case 0.23504 then
bit ==1011
case 0.16543 then
bit ==1100
case 0.10599 then
bit ==1101
case 0.05852 then
bit ==1110
case 0.01936 then
bit ==1111
default:
break
end switch
Bob and Charlie decompresses bit sequence B using Huffman:
DecodeHuffman (F, B) ← Huffman function to decode the bit sequence B
end function
Calculate the total transmission time using Eq. (9).
```

IV. Security Analysis

Any quantum communication protocol that requires to be secured from eavesdropping attempts must pass a security analysis, which is a crucial part of the evaluation process. Security analysis is widely used by researchers to evaluate the security requirements of their protocols and ascertain whether an eavesdropper has a chance to be around [32]–[34]. The security analysis is explained in detail.

A. Man-in-the-Middle Attack

Eve poses as the person with authority to get the information during the MITM attack. The MITM attack is demonstrated in Fig. 5.

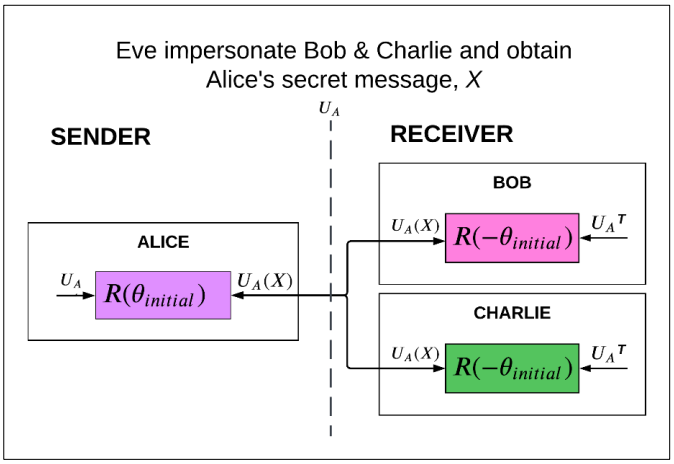

Fig. 5. MITM attack.

Because Eve is unsure of the values of θ_A and Φ, she tries to send a series of fake messages to the receivers. Both θ_A and Φ are secret transformational angles, thus the attacker needs to know both of their values. It is quite challenging for the attacker to determine the precise value because of the secured handshake method used to transmit the information between many parties. Even if Alice gives multiple photons with the same polarisation, Eve cannot get the useful information since a different value of the authentication key is established. Bob can easily decode information X if θ_A and Φ are set to the right values. Eve cannot pretend to be an authorized party if she does not know the authentication key. As indicated in Fig. 5, an authorized party will compare the bits to determine whether an MITM attack has been carried out. For example, Eve might interfere with the communication by continuously interfering with the quantum channel, forcing the authorized parties to restart communication.

B. Beam Splitting Attack

In optical set up, polarizing beam splitters (PBS) are essential elements. As an example, BS are used to merge light beams from several sources into a single optical channel and to randomly pick photons in the detecting subsystems, which in turn determines the measurement basis [35]. PBS are almost always present in front of the detectors in the detection units to split light into its vertically and horizontally polarized components as shown in Fig. 6.

Fig. 6 shows that the beam splitter positioned halfway between Alice, Bob and Charlie in this method, allowing Eve to secretly collect photons. However, Eve has little chance of selecting the appropriate photons to measure because the suggested approach is ineffective for this assault. Eve will have trouble determining the hidden polarisation angles because they will never be made public, even if she is able to collect some of the sent photons without alerting Bob or Charlie. To preserve the level of secrecy and establish unconditional security, the angles of polarisation will also be changed after

numerous photons have been employed with the mutually agreed-upon secret technique [10], [37]. Additionally, the newly updated keys will prevent information about the keys and communications from being sniffed out by eavesdroppers.

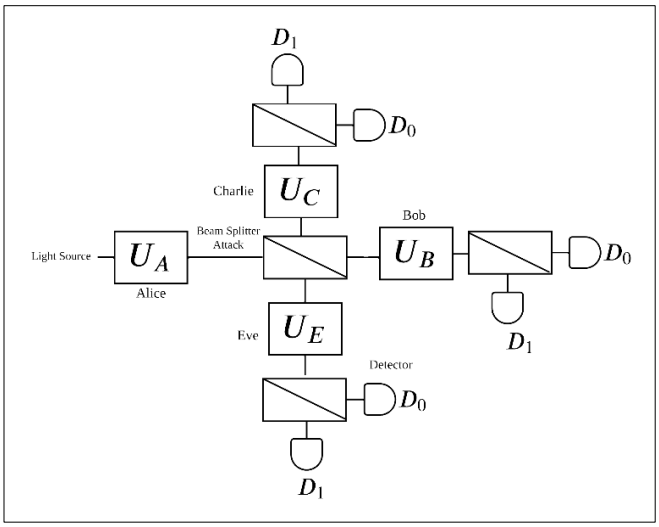

Fig. 6. Beam splitter attack [36].

C. Intercept Resend (IR) Attack

Eve extracts a number of photons that Alice sent and injects the same number of photons into the quantum channel, as seen in Fig. 7.

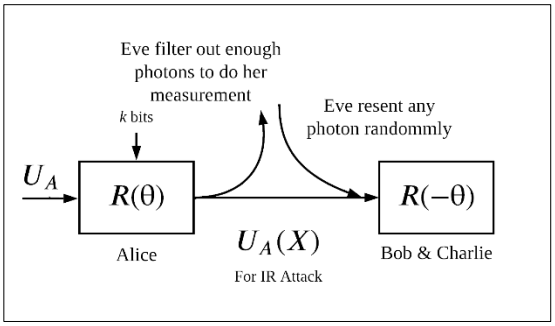

Fig. 7. Intercept resend attack [38].

Fig. 7 illustrates that after Alice has encoded the photons, Eve will try to steal them and replace them with false photons that she has previously prepared. In the proposed E-SSAK protocol, Alice securely and only with Bob and Charlie shares the secret angles θ_A and Φ. Due to her lack of knowledge of the correct values for θ_A and Φ, Eve is unable to measure the intercepted photons precisely. Because quantum states are conveyed in what are known as non-orthogonal states, Eve has limited access to any relevant data. The polarisation angles of photons and security codes create the non-orthogonal quantum states. Additionally, Eve's attempt to figure out the superposition states during the message transformation stage may result in any non-orthogonal states. As a result, no details regarding the polarisation angle are discovered. If Eve was successful in intercepting the sender's sent photons, she will send the photons back to the receiver after doing the measurement. But because Eve is unaware of the polarisation angles and authentication keys that the authorized parties have established, she is unable to breach the protocol. By way of illustration Alice uses the authentication key to encrypt a quantum state of $\psi\rangle = |0\rangle$, in 0^0 of a HWP. Eve won't be able to get the $|\psi\rangle$ since she lacks both the secret polarisation angle and the authentication key. Eve must correctly identify two hidden angles in the suggested protocol. Eve can be recognized if her polarisation angle differs from Alice's and Bob's keys. Since this protocol employs bit-by-bit authentication, Eve cannot examine the statistics of the several photons she receives during her attack without running the risk of being discovered. Eve's attack can be revealed since Alice, Bob and Charlie's measurements on the fake bit differ from those on the actual one.

V. Performance Evaluation

More bits of information will be sent at once with a higher number of levels used for encoding. For example, 2-*d* encoding sends 2 bits at a time, 3-*d* encoding sends 3 bits at a time, 4-*d* encoding, sends 4 bits at a time. The performance of the following evaluation criteria will be used to gauge the success of the simulation experiment.

A. Total Time Taken, T

The QM4SMS protocol was carefully designed and implemented to analyze the time taken to encode the information. Faster transmission times result from increased bit capacity whenever the encoding level is raised. Therefore, it is believed that the transmission process as a whole will significantly improve [22]. Total transmission time includes the time required by HWP to change angles for the transmission of 8 bits of information, which is represented by T_{HWP} , as well as the time required for multiphoton transmission through a quantum communication channel, which is T_{msg} . The time is expressed in seconds. The calculation is made using Eq. (11) as determined by [24].

$$Transmission\ Time = T_{msg} + T_{HWP} \quad (9)$$

A higher number of levels used for encoding will decrease the total HWP turning time required to complete each information transmission process. Therefore, it is believed that the HWP turning time will decrease and contribute to an efficient overall process [13].

B. Noise Tolerance

Most protocol assume the quantum channels to be perfect. However, in a practical implementation, noises in the quantum channel will affect the particles. The security of the suggested protocol in the noisy quantum channel is examined.

Assume that Eve is able to communicate with any party on an ideal channel. Eve performs the intercept-and-resend attack on the qubits being sent from Alice's side to Bob's side in order to obtain Bob's shadow key. She then transmits the intercepted qubits to Bob's side via an ideal channel she has created. Eve may be able to blend her attacks into the quantum channels' background noise by using this strategy [39].

Nevertheless, raising the level of encoding to enhance computing resource comes at a price of increased sensitivity to noise [40].

VI. Result and Discussion

The simulation aimed to investigate the impact of different number of level encoding on total time taken to transmit photon and total received photon with noise.

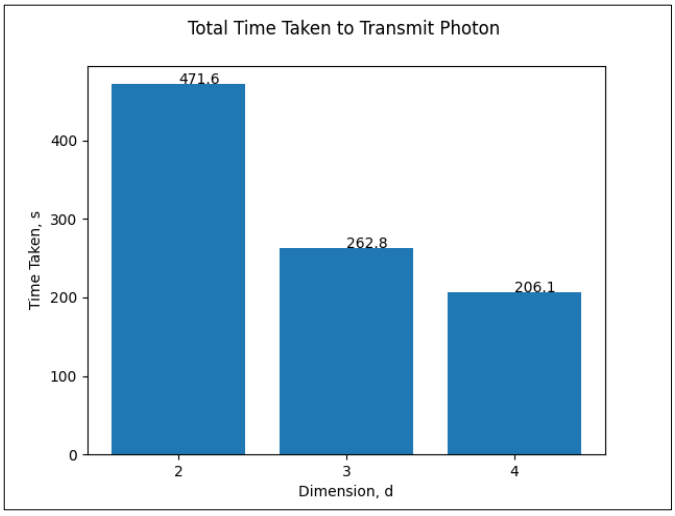

Fig. 8. Total time taken to transmit photon.

Fig. 8 shows the total time taken to transmit photons with different numbers of levels used for encoding, d = 2, 3 and 4. The bar chart above shows a decrease in the time taken to transmit photons when the number of levels used for encoding increases. The 4-*d*, which transfers 4 quantum bits at once, has the fastest photon transmission rate, 206.1 seconds. This is followed by the 3-*d*, which transfers 3 qubits at once, 262.8 seconds, and the 2-*d*, which transfers only 2 qubits at once, has the slowest photon transmission rate, 471.6 seconds. It has been demonstrated that higher levels of encoding can carry more information during each transaction which can speed up the time taken to transmit photons, as stated in [39].

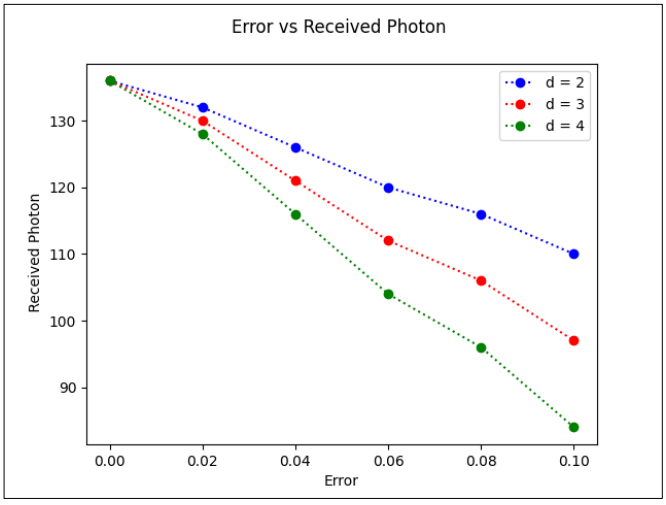

Fig. 9. Total received photon with noise.

Fig. 9 shows the total received photon under the error probability of noisy channels with different levels of encoding. The line graph above shows a decrease in received photons in noisy channels when the size of the level of encoding increases. As can be shown, 4-*d* is beneficial when the error probability of noise is smaller than 0.04. In 0.10, 2- *d* received a higher number of photons than 4-*d*. This is because 4-*d* holds and also loses four quantum bits at once. Compare to 2- *d* which only holds two quantum bits at once and loses 2 quantum bits. It has been demonstrated that the high number of levels used for encoding can carry more information and also lose more information at once, as stated in [29], [40].

In this paper, our benchmark protocol is HBMSS. This is because HMBSS implemented a multiphoton approach in secret message sharing over QSDC and the use of optical devices such as half-wave plates [13]. The other mentioned protocol in Table I was not used as a benchmark because they did not implement optical devices. Nonetheless, this protocol is just for one-to-one communication. Hence, HMBSS does not achieve scalability in terms of the number of parties involved in communication. Therefore, a scalable multiphoton approach is required to enable secure sharing between the legal parties. Other than that, the HMBSS protocol implemented 2-*d*. Which resulted in a low transmission rate. Table VIII shows a comparison of benchmark protocol.

TABLE VIII. Comparison of Benchmark Protocol

Characteristic	**HBMSS** [13]	**Proposed Approach**
Number of levels used for encoding, *d*	2	4
Quantum Cryptography	QSDC	QSDC
Multiparty	No	Yes
Total time taken (sec)	471	206
Photons	Multiphoton	Multiphoton

VII. Conclusion

In conclusion, we presented a new arbitrary protocol that analyzes the performance of the four-level encoding protocol based on sharing the secret message between multiparty by integrating the applications of multiphoton as the information carrier with the QSDC. Information can be exchanged effectively across quantum channels directly using quantum secure direct communications (QSDC). With faster transmission rates and longer photon travel distances, the multiphoton technique is an improved version of the single-photon strategy. Eve has a smaller chance probability to launch an attack when the number of levels used for encoding is increased. High levels of encoding are used in the setup to increase the efficiency of communication since they are more resilient against eavesdropping and could hold more information. We also analyzed the proposed protocol and showed the total time taken to transmit photons when using a high-level encoding. This is because the higher the level of encoding, the more it can transfer or carry quantum bits at once which can speed up the time taken to transmit photons. This paper proves that increasing the level of encoding will provide higher mutual information between the parties involved. Unfortunately, because high-level encoding can hold a lot of information, it also means that a lot of information will be lost under the error probability of a noisy channel. In conclusion, a high number of levels used for encoding brings advantages to quantum cryptography and have its limitation. We believe that

high-level encoding and multiphoton approach among multiparty will play an important role in the next quantum technological leap and overcome the noise as future work.

ACKNOWLEDGMENT

This research was supported by the Ministry of Higher Education (MOHE) through a Fundamental Research Grant Scheme (FRGS/1/2021/ICT11/UTHM/03/1). We also want to thank the Government of Malaysia which provides the MyBrain15 programme for sponsoring this work under the self-funded research grant and L00022 from the Ministry of Science, Technology and Innovation (MOSTI).

REFERENCES

[1] W. Zhang, D. S. Ding, Y. B. Sheng, L. Zhou, B. Sen Shi, and G. C. Guo, "Quantum Secure Direct Communication with Quantum Memory," Phys Rev Lett, vol. 118, no. 22, May 2017, doi: 10.1103/PhysRevLett.118.220501.

[2] Liliana Zisu, Quantum High Secure Direct Communication with Authentication. 2020.

[3] G. L. Long and H. Zhang, "Practical Quantum Secure Direct Communication," in 2020 Cross Strait Radio Science and Wireless Technology Conference, CSRSWTC 2020 - Proceedings, Institute of Electrical and Electronics Engineers Inc., Dec. 2020. doi: 10.1109/CSRSWTC50769.2020.9372501.

[4] Y. Tian, G. Bian, J. Chang, Y. Tang, J. Li, and C. Ye, "A Semi-Quantum Secret-Sharing Protocol with a High Channel Capacity," Entropy, vol. 25, no. 5, May 2023, doi: 10.3390/e25050742.

[5] A. Chandramouli, A. Choudhury, and A. Patra, "A Survey on Perfectly-Secure Verifiable Secret-Sharing," Dec. 2021, [Online]. Available: http://arxiv.org/abs/2112.11393

[6] Y. Liu and Q. Zhao, "E-voting scheme using secret sharing and K-anonymity," World Wide Web, vol. 22, no. 4, pp. 1657–1667, Jul. 2019, doi: 10.1007/s11280-018-0575-0.

[7] M. Blanton, A. Kang, and C. Yuan, "Improved Building Blocks for Secure Multi-Party Computation based on Secret Sharing with Honest Majority," 2020.

[8] N. Z. Harun, "Secured Single Stage Multiphoton Approach for Quantum Cryptography Protocol in Free Space," 2019.

[9] N. S. B. Azahari, N. Z. B. Harun, and Z. B. A. Zukarnain, "Quantum identity authentication for non-entanglement multiparty communication: A review, state of art and future directions," ICT Express. Korean Institute of Communication Sciences, Aug. 01, 2023. doi: 10.1016/j.icte.2023.02.010.

[10] El Rifai et al., "Quantum Secure Communication using Polarization Hopping Multistage Protocols," 2016.

[11] D. Cozzolino, B. Da Lio, D. Bacco, and L. K. Oxenløwe, "High-Dimensional Quantum Communication: Benefits, Progress, and Future Challenges," Advanced Quantum Technologies, vol. 2, no. 12. Wiley-VCH Verlag, Dec. 01, 2019. doi: 10.1002/qute.201900038.

[12] F. Bouchard, R. Fickler, R. W. Boyd, and E. Karimi, "High-dimensional quantum cloning and applications to quantum hacking." Sci Adv. 2017 Feb 3;3(2):e1601915. doi: 10.1126/sciadv.1601915. PMID: 28168219; PMCID: PMC5291699.

[13] N. Z. Harun, Z. A. Zukarnain, Z. M. Hanapi, and I. Ahmad, "Hybrid M-Ary in Braided Single Stage Approach for Multiphoton Quantum Secure Direct Communication Protocol," IEEE Access, vol. 7, pp. 22599–22612, 2019, doi: 10.1109/ACCESS.2019.2898426.

[14] A. Sit et al., "High-dimensional intracity quantum cryptography with structured photons," Optica, vol. 4, no. 9, p. 1006, Sep. 2017, doi: 10.1364/optica.4.001006.

[15] Y. Jo, H. S. Park, S. W. Lee, and W. Son, "Efficient high-dimensional quantum key distribution with hybrid encoding," Entropy, vol. 21, no. 1, Jan. 2019, doi: 10.3390/e21010080.

[16] M. De Oliveira, I. Nape, J. Pinnell, N. Tabebordbar, and A. Forbes, "Experimental high-dimensional quantum secret sharing with spin-orbit-structured photons," Phys Rev A (Coll Park), vol. 101, no. 4, Apr. 2020, doi: 10.1103/PhysRevA.101.042303.

[17] C. Sekga, M. Mafu, and M. Senekane, "High-dimensional quantum key distribution implemented with biphotons," Sci Rep, vol. 13, no. 1, Dec. 2023, doi: 10.1038/s41598-023-28382-w.

[18] Y. Ding et al., "High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits," npj Quantum Inf, vol. 3, no. 1, 2017, doi: 10.1038/s41534-017-0026-2.

[19] B. Ndagano et al., "A deterministic detector for vector vortex states," Sci Rep, vol. 7, no. 1, Dec. 2017, doi: 10.1038/s41598-017-12739-z.

[20] O. Elmabrok and M. Razavi, "Wireless quantum key distribution in indoor environments," Journal of the Optical Society of America B, vol. 35, no. 2, p. 197, Feb. 2018, doi: 10.1364/josab.35.000197.

[21] R. Mueller, D. Ribezzo, M. Zahidy, L. K. Oxenløwe, D. Bacco, and S. Forchhammer, "Efficient Information Reconciliation for High-Dimensional Quantum Key Distribution," Jul. 2023, [Online]. Available: http://arxiv.org/abs/2307.02225

[22] N. S. Azahari and N. Z. Harun, "Quantum Cryptography Experiment using Optical Devices," 2023. [Online]. Available: www.ijacsa.thesai.org

[23] P. K. Verma, M. El Rifai, and K. W. C. Chan, "Multi-photon Quantum Secure Communication," 2019. [Online]. Available: http://www.springer.com/series/4748

[24] N. Z. Harun, Z. A. Zukarnain, Z. M. Hanapi, I. Ahmad, and M. F. Khodr, "Multiphoton quantum communication using multiple-beam concept in free space optical channel," Symmetry (Basel), vol. 13, no. 1, pp. 1–16, Jan. 2021, doi: 10.3390/sym13010066.

[25] E. Hecht, "Optics Fifth Global Edition ," Pearson. Accessed: Nov. 13, 2022. [Online]. Available: https://www.academia.edu/44107964/OPTics_FiFTh_EdiTiON_GlObAl_EdiTiON

[26] Z. Li et al., "Three-Channel Metasurfaces for Multi-Wavelength Holography and Nanoprinting," Nanomaterials, vol. 13, no. 1, p. 183, Dec. 2022, doi: 10.3390/nano13010183.

[27] E. Hecht, "Optics: A Contemporary Approach to Optics with Practical Applications and New Focused Pedagogy, Global edition," p. 725, 2017, Accessed: Nov. 13, 2022. [Online]. Available: https://www.pearson.com/uk/educators/higher-education-educators/program/Hecht-Optics-Global-Edition-5th-Edition/PGM1095066.html

[28] Xiang Li, Kejia Zhang, Long Zhang, and Xu Zhao, "A New Quantum Multiparty Simultaneous Identity Authentication Protocol with the Classical Third-Party," 2022.

[29] M. El Rifai, N. Punekar, and P. K. Verma, "Implementation of an m-ary three-stage quantum cryptography protocol," in Quantum Communications and Quantum Imaging XI, SPIE, Sep. 2013, p. 88750S. doi: 10.1117/12.2024185.

[30] C. Lee et al., "Large-alphabet encoding for higher-rate quantum key distribution," Opt Express, vol. 27, no. 13, p. 17539, Jun. 2019, doi: 10.1364/oe.27.017539.

[31] I. Vagniluca et al., "Efficient Time-Bin Encoding for Practical High-Dimensional Quantum Key Distribution," Phys Rev Appl, vol. 14, no. 1, Jul. 2020, doi: 10.1103/PhysRevApplied.14.014051.

[32] Y. Chang, S. Zhang, L. Yan, and J. Li, "Deterministic secure quantum communication and authentication protocol based on three-particle W state and quantum one-time pad," Chinese Science Bulletin, vol. 59, no. 23, pp. 2835–2840, 2014, doi: 10.1007/s11434-014-0333-3.

[33] A. A. A. El-Latif, B. Abd-El-Atty, M. S. Hossain, S. Elmougy, and A. Ghoneim, "Secure quantum steganography protocol for fog cloud internet of things," IEEE Access, vol. 6, pp. 10332–10340, Jan. 2018, doi: 10.1109/ACCESS.2018.2799879.

[34] H. Li, D. Li, X. Zhang, G. Shou, Y. Hu, and Y. Liu, "A Security Management Architecture for Time Synchronization towards High Precision Networks," IEEE Access, 2021, doi: 10.1109/ACCESS.2021.3107203.

[35] L. O. Mailloux, M. R. Grimaila, D. D. Hodson, and G. Baumgartner, "Performance Evaluations of Quantum Key Distribution System Architectures," 2015. [Online]. Available: www.computer.org/security

[36] C. Caputo, M. Simoni, G. A. Cirillo, G. Turvani, and M. Zamboni, "A simulator of optical coherent-state evolution in quantum key distribution systems," Opt Quantum Electron, vol. 54, no. 11, Nov. 2022, doi: 10.1007/s11082-022-04041-8.

[37] Darunkar and A. Bhagyashri, "Multi-photon Tolerant Quantum Key Distribution Protocol for Secured Global Communication," 2017.

[38] N. Z. Harun, "Secured Single Stage Multiphoton Approach for Quantum Cryptography Protocol in Free Space Optic," University Putra Malaysia, 2019.

[39] R. G. Zhou, M. Huo, W. Hu, and Y. Zhao, "Dynamic Multiparty Quantum Secret Sharing with a Trusted Party Based on Generalized GHZ State," IEEE Access, vol. 9, pp. 22986–22995, 2021, doi: 10.1109/ACCESS.2021.3055943.

[40] C. Reimer et al., "High-dimensional one-way quantum processing implemented on d-level cluster states," Nature Physics, vol. 15, no. 2. Nature Publishing Group, pp. 148–153, Feb. 01, 2019. doi: 10.1038/s41567-018-0347-x.