IAC-23,B2,3,5,x79705

Secure CubeSat-to-CubeSat Communication using Quantum Key Distribution for Information Updates and Risk Alerts

Priyank Dubey[a b], **Andreas M. Hein** [c]

[a] *Visiting Student, SpaSys-SnT, University of Luxembourg, Luxembourg* . priyank.dubey@ext.uni.lu
[b] Corresponding Author
[c] *Associate Professor, SpaSys-SnT, University of Luxembourg, Luxembourg* . andreas.hein@uni.lu

Abstract

With the growing use of CubeSats for various applications, such as remote sensing, communication, and scientific research, the need for secure communication between them has become crucial. CubeSat-toCubeSat communication is becoming increasingly important for maintaining the security and reliability of CubeSat missions in modern day. CubeSats often carry sensitive information that must be protected from unauthorized access or interception and hence vulnerable to physical and cyber-attacks that could compromise their security. In this paper, we propose a system for secure CubeSat-to-CubeSat communication using Quantum Key Distribution (QKD). It consists of a photon source, polarization manipulation device for quantum state preparation and photon detectors with the capability of quantum state measurement. This system could enable CubeSats to update each other in real-time on conditions and status, allowing for rapid response to potential risks. Apart from this, it also allows CubeSats to operate independently in space without relying on ground stations or other infrastructure for communication. In the method, the information to be shared is first encoded into binary signals, and then the sender CubeSat (Alice) generates a stream of single photons with binary codes represented by randomly chosen polarization states of photons and sends them to the receiver CubeSat (Bob). The receiver CubeSat measures the polarization of each photon and communicates its measurements back to Alice. Alice and Bob can then use the measurement results to establish a shared secret key. As the polarization state of a photon is inherently random, any attempt to eavesdrop on the communication will inevitably alter the state of the photons, which can be detected by Alice and Bob. By using this method, CubeSats in a network can exchange information securely and effectively, ensuring the reliability and stability of the CubeSat network.

Keywords: Quantum computing for space, Space technology, Quantum communication for satellite constellation , CubeSat-CubeSat communication, CubeSat constellation, Quantum algorithms for aerospace

1. Introduction

CubeSats are standardized and cost-effective platform, which were developed by California Polytechnic State University and Stanford University with the aim of offering university students practical exposure to satellite technology. The fundamental unit is denoted as a 1U cube, with dimensions of 10x10x10 cm and a mass of around 1 kilograms. Over the course of its development, CubeSats have undergone several adaptations, resulting in the emergence of multiple configurations like as 2U, 3U, 6U, and even 12U, in order to facilitate the execution of more complex missions and the integration of advanced payloads [1]. CubeSats are a class of spacecraft known as miniature satellites, which are classified according to their dimensions, specifically mini-satellites, micro-satellites, nano-satellites, pico-satellites, and femto-satellites [2]. CubeSats offer a diverse range of applications, including educational objectives, scientific investigations, Earth observation, communication capabilities, technology validation, and space exploration. They have the capability to function as communication relays, facilitate the testing of novel space technologies, and serve as supplementary components for more extensive missions [3]. Nevertheless, because to their constrained dimensions and limited capabilities, it becomes essential to develop innovative methods in order to fulfill mission objectives. The increase in the number of CubeSats gives rise to concerns regarding the building up of space debris [4].

Because of its low cost, a constellation of hundreds of CubeSats becomes an economical and commercially viable service [5] [6]. There are two distinct approaches that have been pursued in the context of CubeSat constellations. The first is to improve coverage or revisiting frequency by increasing the quantity of satellites within the constellation. In this approach, all satellites within the constellation are equipped with identical payloads and perform comparable func-

tions [7] [8]. Another approach involves utilizing a constellation consisting of numerous CubeSats, each equipped with distinct distributed payloads, in order to execute a cohesive mission or provide a comprehensive service. The previous method has been extensively demonstrated and investigated, but the latter direction focuses more on distributed payloads or the utilization of many functional satellites to construct a constellation that may deliver integrated services. This approach has garnered increasing attention within the space industry [9][10][11].

The security of space vehicles has emerged as a subject of growing interest and discussion within technical and governmental organizations [12]. The matter of cybersecurity has long been a concern for space systems involved in defense or intelligence activities. From the CubeSat perspective, they often carry sensitive information that must be protected from unauthorized access or interception and hence vulnerable to physical and cyber-attacks that could compromise their security [13][14]. Traditional communication system relies on classical communication principles. Although these systems have demonstrated efficacy and dependability over an extended period, they include inherent vulnerabilities to eavesdropping and various cyberattacks. This susceptibility is particularly pronounced in light of technological advancements and the increasing sophistication of hostile actors. Hence, posing security threats and reliability of sensitive information carried by a spacecraft [15].

Quantum communication, which is based on the fundamental principles of quantum physics, presents a highly promising approach for establishing secure and reliable communication channels between spacecrafts. In contrast to classical communication techniques that rely on classical bits, quantum communication exploits quantum bits, commonly known as qubits, which can exist in a superposition of states. This distinctive characteristic has notable benefits, particularly with in terms of security. One of the most fascinating phenomena observed in the field of quantum communication is known as *entanglement* which refers to the interconnection of particles [16]. Entangled particles exhibit a phenomenon wherein their states remain interconnected, despite being physically separated by significant spatial distances. Modifications to the state of a single particle will result in immediate and simultaneous alterations to the state of the other particle. This phenomenon plays a pivotal role in numerous quantum communication procedures. One of the most prominent applications of quantum communication is Quantum Key Distribution (QKD) [17].

The exploitation of QKD to develop a space-based communication system is an active research area. Several free-space as well as satellite-to-ground communication system using QKD have been proposed [18][19][20][21][22]. In [23], a CubeSat based QKD system was developed for down linking strongly attenuated light pulses with encoded quantum information for encryption keys. Similarly, SpooQySats is a program developing photon pair sources using CubeSat nanosatellites for satellite-based quantum key distribution (QKD)for secure uplinks and downlinks, and establishing a global space-based quantum key distribution network [24]. In [25], CubeSats constellation is proposed and the corresponding analysis is done for establishing QKD based communication in UK. These studies mainly focuses on the photonic based QKD when CubeSat are in line of sight. However, it is not always possible for CubeSat constellation to be aligned in a specific manner. These studies also lacks the secure quantum protocol for CubeSat constellation.

In the present investigation, we architect a CubeSat network fortified by entanglement-based Quantum Key Distribution (QKD), augmented by quantum repeaters with quantum memory capabilities for enabling entanglement swapping. We introduce a customized protocol grounded in Dynamic Quantum Secret Sharing (DQSS), explicitly designed for ensuring secure data exchanges between CubeSats. Detailed system architecture is elaborated, highlighting key components such as sources of entangled photons, detection mechanisms, devices for polarization manipulation, and photon detectors. Our proposed framework is tailored for a constellation of CubeSats, each equipped with essential space systems alongside specialized quantum hardware, including entangled photon sources and quantum memory. The framework presupposes the presence of entangled photon pair sources situated between neighboring CubeSats in the constellation. The study explores two specific use-cases: the detection of incoming orbital space debris by CubeSats and the reception of such information from Ground Stations. We outline the methodologies for risk assessment, its conversion into a binary format, and subsequent encoding into photon polarization states for secure communication. Additionally, we illustrate the operational modalities for CubeSat-to-CubeSat communication and address the network's dynamic capabilities. Specifically, we demonstrate that the network can seamlessly integrate newly launched CubeSats or remove existing ones without compromising the integrity of the overall constellation. To substantiate the practicality and robustness of our approach, we present evaluations on system efficiency and security metrics.

This paper is structured as follows: In Sect. 2, we provide an basic introduction to system architecture by briefly defining various subsystems such as Entangled Photon Source, detection system, Entanglement Switch and Quantum Memory. We have discussed about the step by step implementation methodology in Sect. 3. In Sect. 4, we discuss the efficiency and security of the proposed system. In Sect. 5, we finally conclude the paper with the conclusion.

2. System Architecture

In this section, we address general considerations on the organization of an entanglement-based QKD network of CubeSat as shown in Fig. 1. Furthermore, we provide a comprehensive analysis of the specific space component of the network, followed by an in-depth examination of the current advancements in crucial components and the standardization processes.

We assume a standard constellation of CubeSats in a certain orbit, such that each of these CubeSat shares entanglement with their adjacent neighboring satellites. The satellites transmit pairs of entangled photons towards their neighbours. Each CubeSat consists of a payload and a platform. The payload consists of the Entangled Photon Source (EPS), two optical terminals, and a processor. Entangled photon pairs are produced by the source in one of the four Bell states. The source includes a monitoring module that measures the transmitted quantum state fidelity, throughput, as well as the optical, thermal, and mechanical status of the source. The on-board optical terminal consists of two telescopes that are used to route each photon of an entangled pair towards the neighboring satellites. The telescopes are attached to remote control actuators designed for the purposes of Pointing, Acquisition, and Tracking (PAT), which are commonly directed by beacon lasers. The payload processor is responsible for analyzing commands, monitoring the state of the source (including power, optical, thermal, etc.), and optionally managing a laser master clock to synchronize with the ground for precise time-stamping at a sub-nanosecond scale. In addition, the payload processor enhances the optimization of the encoding variable correction and guarantees the self-calibration of the PAT device.

The platform comprises several essential components, namely solar panels, batteries, an onboard processor, a memory unit, a radio terminal for Telemetry, Tracking and Control (TTC), sensors for satellite trajectory and attitude determination, actuators for adjusting the satellite attitude, thrusters, and a GNSS receiver. The platform is responsible for the management of energy resources, such as solar panels and batteries. It also performs the crucial functions of protecting and stabilizing the payload against many factors, including heat, space debris, radiations, and vibrations. Additionally, the platform ensures the maintenance of the satellite's altitude and attitude. The platform facilitates the transmission of telemetry data and the reception of commands from the control segment. Additionally, it enables the handling of faults and the execution of deorbiting procedures at the conclusion of the satellite's operational lifespan.

The entanglement photon source and detection system is based on the studies [26][27] as depicted in Figure. 2. The source generates pairs of photons with distinct wavelengths (non-degenerate) that are entangled in terms of their polarization state. When the detection unit within the science instrument measures one photon from each pair, specifically the idler photon at a wavelength of 837 nm, the other photon, known as the signal photon at a wavelength of 785 nm, is transmitted to the ground along with a time beacon through the optical ground station interface. A minute proportion of the signal photons, nonetheless, undergoes analysis within the self-check unit of the detection system of the scientific instrument to assess the quality of entanglement and internal efficiency. A dichroic mirror is utilized to segregate idler and signal photons, enabling their detection on board and on the ground, respectively. During the analysis process, all idle photons are examined within the scientific instrument. However, the signal photons (together with the beacon) are divided using a non-polarizing beam splitter, with approximately 90% of them directed towards the interface of the optical ground station. The fraction of signal photons that remain are then evaluated in the self-check unit. Let us describe each component in details:

2.1. Entangled Photon Source

Entangled states are generated inside a beam displacement interferometer through the use of two pump beams with orthogonal polarization. These beams undergo down-conversion within a periodically poled crystal, and subsequently, they are joined together [28]. The pump beam with a wavelength of 405 nm traverses a series of optical components in its path. These components include a prism pair for aligning the beam, a lens for focusing it onto the periodically poled crystal, a filter to eliminate fluorescence, a unit consisting of a half-wave plate and a polarizing beam splitter for adjusting the beam's intensity, and another half-wave plate to rotate the polarization to an angle of 45° prior to entering the interferometer. In a beta barium borate (BBO) crys-

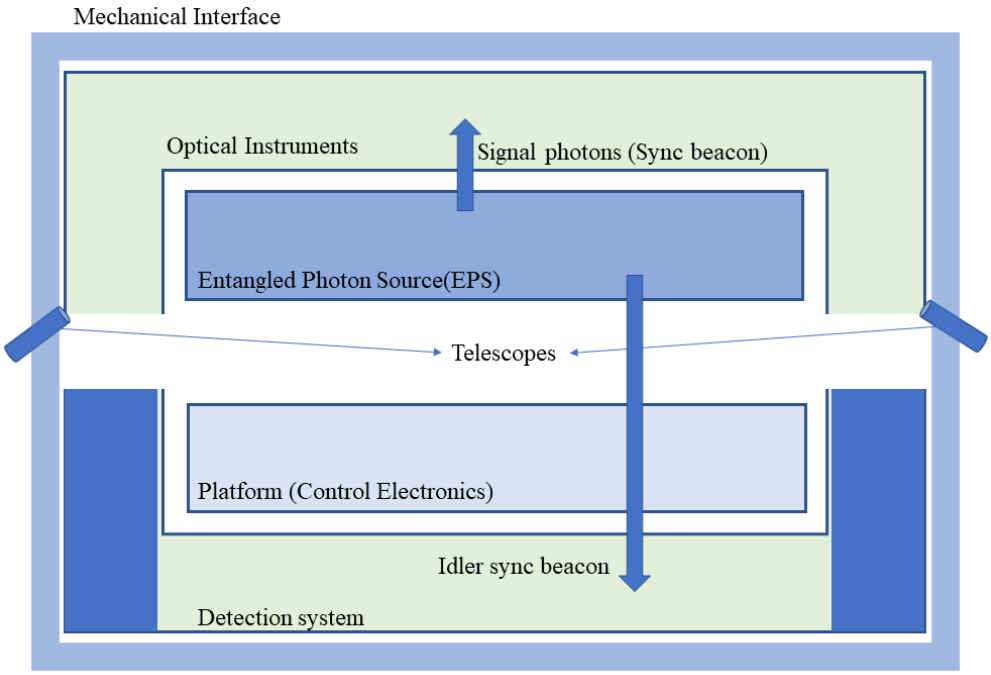

Figure 1: Symbolic depiction of major subsystem of architecture for entanglement-based QKD net- work of CubeSat constellation.

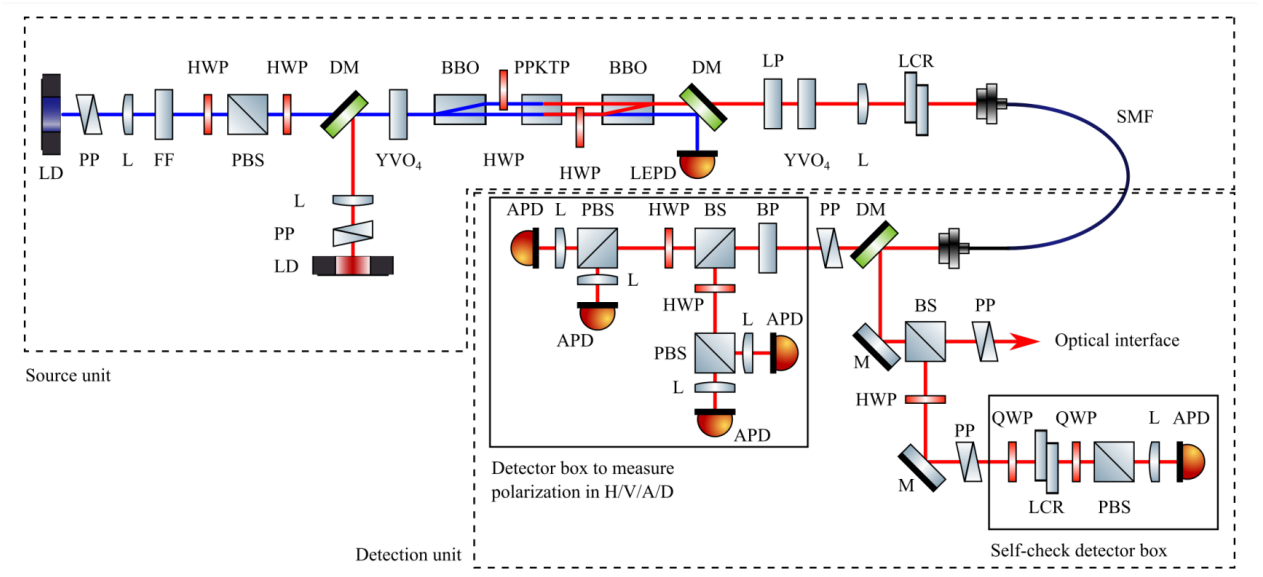

Figure 2: Schematic of the mechanism and components behind the sending and detection unit. LD: laser diode; PP: prism pair; L: lens; FF: fluorescence filter; HWP: half-wave plate; PBS: polarizing beam splitter; DM: dichroic mirror; YVO4: yttrium orthovanadate; BBO: beta barium borate; PPKTP: periodically poled potassium titanyl phosphate; LEPD: lateral effect photodiode; LP: long pass filter; LCR: liquid crystal retarder; SMF: single-mode fiber; BP: band pass filter; BS: beam splitter; APD: avalanche photodiode; M: mirror; QWP: quarter-wave plate. [26][27]

tal, the horizontally and vertically polarized pump beam undergo spatial separation. The beam with horizontal polarization is subsequently transformed into vertical polarization using a half-wave plate. Both beams are then subjected to down-conversion within a temperature-stabilized periodically poled potassium titanyl phosphate (PPKTP) crystal. The daughter photons, specifically the idler photon with a wavelength of 837 nm and the signal photon with a wavelength of 785 nm, exhibit vertical polarization that is identical to that of the pump photons in the context of SPDC Type-0. The polarization of one beam is transformed into a horizontal orientation prior to the recombination of both beams into a subsequent BBO crystal. The residual pump light is eliminated using a dichroic mirror and a long pass filter. Subsequently, the down-converted beam is rendered collimated through the utilization of a secondary lens. In order to account for variations in wavelength and route length within the nonlinear crystals, a configuration involving two yttrium orthovanadate (YVO4) crystals arranged in an interferometer sandwich is employed. Furthermore, a liquid crystal retarder (LCR) is employed, positioned behind the collimating lens within the source unit, in order to actively manipulate the phase relationship between the signal and idler.

2.2. Detection System

In terms of detection, the signal and idler are initially separated through the use of a dichroic mirror. This separation allows for the signal to be detected on board, while the idler is sent towards a another reciver CubeSat. The beam known as the idler is passed via the dichroic mirror. It is then aligned with a pair of prisms and undergoes filtering. The polarization of the beam is afterwards recorded in four standard channels, namely horizontal (H), vertical (V), anti-diagonal (A), and diagonal (D). The beam splitter, which has a 50/50 probability of selecting the measurement basis (H/V or A/D), utilizes a combination of a half-wave plate and a polarizing beam splitter to project the photons onto their respective states. The process of measurement involves directing the light onto avalanche photodiodes (APDs). The signal beam, after being reflected by the dichroic mirror, is initially divided to facilitate its transmission to a receiver located on the neighbouring CubeSats and its subsequent analysis conducted on it. Approximately 90% of the signal photons are directed towards the receiving CubeSat, while the remaining portion is allocated to a self-check detector unit. This unit serves the purpose of quantifying the quality of entanglement and the efficiency involved.

2.3. Entanglement Switch and Quantum Memory

The entanglement switch is a component situated within each CubeSat, designed to facilitate the transmission of entanglement to one of multiple alternative CubeSats through the process of entanglement switching. The entanglement switches are interconnected through a combination of a quantum channel, which facilitates the exchange of entangled qubits, and a classical channel, which enables synchronization, heralding, and unitary rectification through local operations and classical communications. The fundamental component of an entanglement switch is a Bell-state measurement apparatus, which concurrently measures the state of one photon received from each of the two neighboring CubeSat. This measurement process serves to entangle the remaining photons within each respective link. It is assumed that each entanglement switch is equipped with a quantum memory (QM) to store the resource and facilitate delayed switching to a neighboring node upon request [29]. Additionally, it is assumed that there exists a source of entangled photon pairs situated between each CubeSats in the constellation. This source is responsible for generating the quantum channel and is an integral component in establishing the elementary linkages within the network .

The receiver CubeSat can either directly serve end users or perform entanglement routing between two distant CubeSats. Each CubeSat is composed of an optical terminal, a quantum receiver, an entanglement processor, an entanglement storage unit, potentially a radio terminal, a secured classical network interfaced to other CubeSats in constellation, and an entanglement switch at the interface with the local network or between elementary Space links, all hosted in a optical terminal. Photons are collected though a telescope equipped with a PAT device, and their states are finally stored in a QM until an entanglement swapping is performed to extend entanglement relationships and build end-to-end connections. The storage of entangled states allows the non-real-time and on-demand usage of the entanglement resource provided by the CubeSats. This key aspect ensures continuous secure communication with available entanglement resources for end-users, independently of satellite availability and weather fluctuations that momentarily compromise optical communications in space.

3. Methodology

In this section, we outline the methodology of secure CubeSat-to-CubeSat Communication using entanglement based QKD for information Updates and risk alert. As mentioned in earlier sections, we consider a small constellation of CubeSats in a certain orbit. Each CubeSat is deigned as described in the Section. 2 meaning that each CubeSat in the constellation is equipped with basic space system unit along with the entangled photon source, detection system, entanglement switch and quantum memory. We also assume that the CubeSats in the constellation are connected with classical network along with sharing entangled pairs with the neighbouring CubeSats. In order to provide the methodology of proposed concept, we assume the following cases for information updates and risk alerts: Case (i) Incoming Orbital Space Debris as detected by CubeSats through onboard sensors (Figure. 4). Case (ii) Information about incoming orbital space debris as provided by Ground Station(GS) to one of the CubeSat which are in the communication window of GS (Figure. 3). In the upcoming subsections, we will consider these cases to develop the methodology:

3.1. Risk Detection

As mentioned above, we will assume orbital space debris as risk. Space debris tracking is crucial for the safe operation of satellites and other spacecraft. While ground-based radar and telescopes are widely utilized for this purpose, onboard cameras and sensors provide an additional degree of protection and real-time tracking capabilities [30]. The problem of detecting space debris becomes considerably more complex in a satellite constellation due to the sheer number of satellites involved, but it also gives an opportunity for improved situational awareness. Each satellite can act as a node in a networked system for comprehensive trash tracking by using onboard technology such as optical cameras in the visible and infrared spectra, Lidar, and accelerometers. These sensors can be built to function with little power consumption, fitting into the restricted energy budgets typical of most satellites.

The acquired data is initially processed onboard using object detection algorithms to remove potential debris from celestial bodies and other satellites [31]. Tracking algorithms then forecast the paths of these items to determine the likelihood of a collision [32]. Importantly, data from separate satellites can be merged at a single node or spread over the network for more accurate tracking and prediction. This data fusion not only improves the tracking system's robustness, but also enables for real-time updates, which are required for quick collision-avoidance judgments [33][34]. One of the key operational considerations is the real-time nature of the tracking system. Given that communication with ground stations can be intermittent or delayed, each satellite should have the capability for autonomous operation.

There are several studies which look into this problem. In [35], authors examined ground-based tracking, satellite-based, simulation-based, and fusion-based detection techniques, with the fusion-based method being particularly effective in detecting debris in both sunlit and non-sunlit areas. [36][37][38]presents a image-based control scheme for tracking space debris using onboard optical sensors using Kalman filter to reduce camera noise, detects debris path, and estimates angular velocity. While [39] presents an presents an original architecture for relative navigation using a single passive camera to reconstruct the relative state between a chaser spacecraft and a known target.

The tracking of space debris from ground stations predominantly depends on the utilization of advanced radar equipment and optical telescopes. The aforementioned installations are deliberately positioned across several locations worldwide in order to ensure extensive surveillance of Earth's orbital space [40]. Radar devices have shown to be highly efficient in monitoring tiny debris within low Earth orbit by producing radio waves that reflect off objects and subsequently return to the base station [41]. Through the analysis of the signals that are received, the station is able to derive information regarding the dimensions, velocity, and path of the object. Optical telescopes serve as a valuable complement to radar systems, particularly in the context of monitoring objects located in higher orbits that are less amenable to radar detection. These telescopes employ the technique of capturing the reflected light from debris in order to ascertain the precise position and velocity of the object. Sophisticated algorithms are employed to analyze the data obtained from these sensors in order to forecast the trajectories of debris and detect possible instances of collision with operational satellites [42][43]. The acquisition of this data is crucial for the purpose of mission planning and the execution of collision avoidance measures. Ground stations frequently engage in collaborative efforts, wherein they exchange data and computational resources with the aim of enhancing tracking precision and prediction capacities. In the realm of space debris management, ground-based tracking continues to serve as a fundamental pillar.

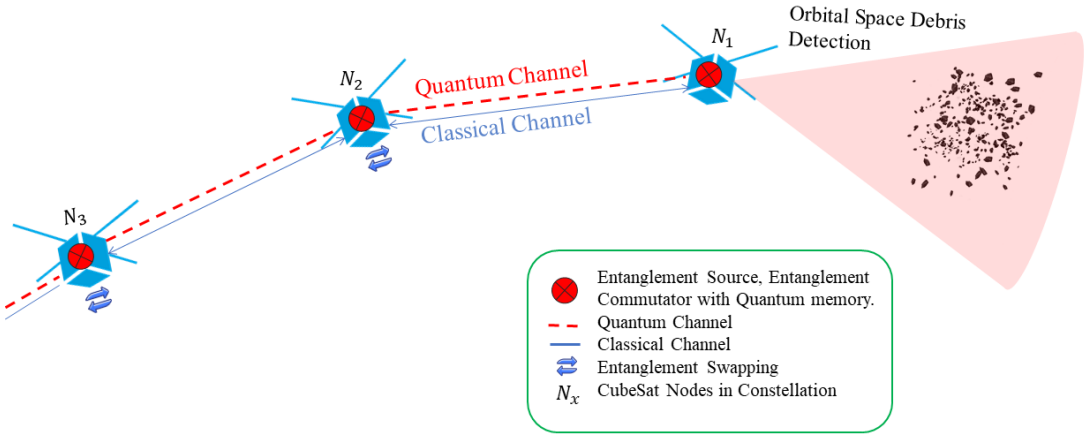

Figure 3: Architecture for entanglement based QKD system for CubeSat constellation where on-board detection system is providing risk alerts, which can be further communicated securely to other CubeSat by utilizing entanglement.

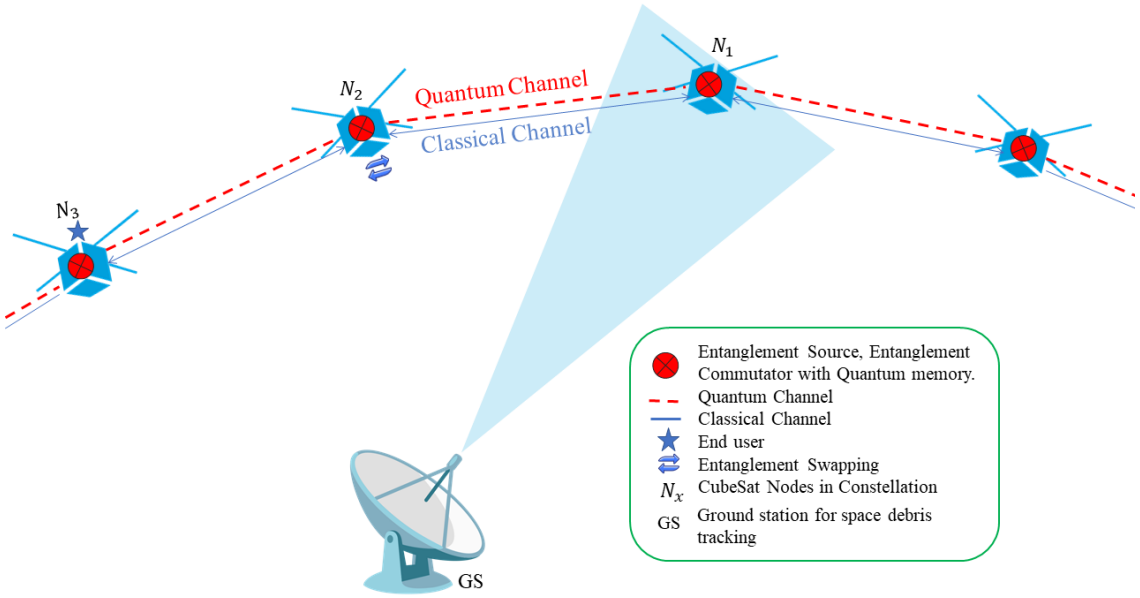

Figure 4: Architecture for entanglement based QKD system for CubeSat constellation where ground station is providing risk alerts to one of the CubeSat in its communication window, which can further communicate this information securely to other CubeSat by utilizing entanglement swapping.

3.2. Data Encoding

After the risk detection, the next step is data encoding for further transfer. The conversion of information into binary signals is a fundamental component of digital communication and computing. During this process, numerous types of data—from text and numbers to images, audio, and video—are converted into 0s and 1s sequences. Text characters, for example, could be represented using ASCII encoding [44], in which each letter or symbol corresponds to a distinct binary sequence. Numerical data can be translated straight to binary form, with techniques such as two's complement employed to represent negative integers. The color of each pixel or the loudness of each audio sample is turned into a binary number in multimedia data such as photos and sounds. constant-length encoding, in which each data unit is represented by a constant number of bits, or variable-length encoding, in which the number of bits varies dependent on particular conditions, such as the frequency of a character in a text [45]. Once the data has been encoded into binary, the sender CubeSat, let's call it Alice, takes the process a step further by transmitting data using photon quantum characteristics by using quantum Encoding with Polarization States as described in Section.2.1. In this example, Alice produces a stream of single photons, each carrying a piece of the binary-encoded data. The polarization states of these photons represent binary codes. A horizontally polarized photon, for example, may represent a binary 0, whereas a vertically polarized photon may represent a 1.

3.3. Basic Concept of Operation

As depicted in Fig. 4 and 3, we propose a simple operational scenario demonstrating the processing of information updates or warnings between two CubeSats Alice N_1 and Bob N_3. Before any communication request from Alice or Bob, the network generates entanglement resources on elementary lines and saves them in QM at each intermediate CubeSat(N_2). After detecting the hazard, processing it, and interpreting its impact on the individual or group of satellites. The host CubeSat can play the role of AliceN_1, while the target CubeSat/CubeSats can play the role of BobN_3. When two end-users, in this case Alice and Bob, send a communication request, the on-board controller determines the best path to connect them and organizes entanglement swapping along that path. A Bell state measurement enables entanglement swapping at the switches N_2 and thus the weaving of an end-to-end entanglement link. Entanglement follows the red path, which is made up of three satellites and one entanglement switch. The entanglement resource on each link will be consumed to build the end-to-end entanglement, and the end-to-end entanglement will be consumed at the time of communication between Alice and Bob, for example, when Alice teleport her qubit state to Bob.

3.4. Protocol for secure QKD

In this section, the Dynamic Quantum Secret Sharing protocol (DQSS) tailored for secure information updates among CubeSats is deigned. The designed protocol offers secure information transfer as well as it provides network dynamism, which means that a newly launched CubeSat can be added to the constellation network, and a CubeSat can be removed from the constellation network without affecting the entire network. The protocol will accommodate both cases where Alice and Bob are adjacent and when they have intermediate CubeSats in between.

Notations: K_X : n-bit symmetric quantum key associated with CubeSat X. K_M : Master key held by the central CubeSat (Alice). $\oplus$: Bitwise XOR operation for key updates. ϕ_{XY} : Entangled quantum state between CubeSats X and Y.

Step 1: The CubeSat which detected the hazard will act as Alice (transferring CubeSat). It will maintain and distribute the master key K_M.

Step 2: For Adjacent CubeSats - Initial Key Generation and Master Key Setup. Alice performs a entanglement based QKD protocol (E91 or the BBM92) with each adjacent CubeSat (e.g., Bob, Charlie) to generate an n-bit symmetric key K_{AliceBob} , $K_{\text{AliceCharlie, etc.}}$. Alice calculates the initial master key as follows:

$$K_M = K_{\text{AliceBob}} \oplus K_{\text{AliceCharlie}} \oplus \cdots$$

Step 3: For non-adjacent CubeSats - entanglement swapping for Key Generation. Charlie performs a Bell-state measurement on his part of $\phi_{\text{AliceCharlie}}$ and $\phi_{\text{CharlieBob, }}$, effectively entangling Alice and Bob. Alice and Bob can now derive a shared secret key K_{AliceBob} through the entangled state.

Step 4: Master Key Update - Dynamic Addition of a New CubeSat (David). A new CubeSat, David, is introduced into the network. Alice generates a new symmetric key $K_{\text{AliceDavid}}$ with David using a quantum protocol. The master key is updated as follows:

$$K'_M = K_M \oplus K_{\text{AliceDavid}}$$

Alice securely communicates K'_M to all existing CubeSats for future secure communication.

Step 5: Master Key Update - Dynamic Removal of a CubeSat. Suppose a CubeSat, say Charlie, leaves the network. Alice updates the master key:

$$K''_M = K'_M \oplus K_{\text{AliceCharlie}}$$

Alice securely sends the updated K''_M to the remaining CubeSats.

Step 6: Secure Communication using Entanglement. For added security, Alice generates and shares entangled states ϕ_{XY} with each adjacent CubeSat. Non-adjacent CubeSats utilize entanglement swapping to establish a secure channel.

Step 7: Information Update and Secure Communication. For normal information updates, CubeSats use the latest master key K_M or individual keys K_X depending on the security requirements. When network changes occur (like adding or removing a CubeSat), Alice sends a secure message to all CubeSats to confirm the change and update the master key.

4. Efficiency and Security of Proposed Scheme

The efficiency of quantum communication protocols is calculated using two related but distinct parameters. The first is easily defined as

$$\eta_1 = \frac{c}{q} \tag{1}$$

where c is the total number of classical bits (message bits) transmitted/shared via the protocol and q is the total number of qubits employed for the purpose [46][47].

In this context, it is necessary to establish a precise delineation of the maximum value that η_1 can attain within the framework of DQSS protocols. In order to facilitate comparison with previous approaches, we examine a multi-party DQSS scheme consisting of m parties, with Alice serving as the principal and $(m1)$ agents. Alice is now tasked with implementing a sub-protocol with each of the aforementioned agents. The maximum efficiency for each of these sub-protocols can be 0.5[48]. This phenomenon occurs when a pair of $2x$ qubits, consisting of a combination of verification qubits and message qubits, traverse a quantum channel that can be accessed by an eavesdropper named Eve. To assess the possibility of eavesdropping, a subset of x qubits is utilized. In this scenario, for any given value of δ greater than zero, the likelihood of obtaining fewer than δn errors on the verification qubits, while simultaneously obtaining more than $(\delta + \epsilon)n$ errors on the remaining x qubits, approaches a value that is significantly smaller than $e^{-O(\epsilon^2 x)}$ as x becomes large [48]. In order to guarantee the absolute security of the sub-protocol employed by Alice and her ith agent of level 1, it is necessary for them to conduct a thorough examination of fifty percent of the sent qubits to detect any potential eavesdropping attempts.

Thus $\eta_{1\,\max} = 0.5$ and it is easy to interpret that in m-party DQSS, Alice prepares a 1-bit secret or key $K_M = K_{A_1} \oplus K_{A_2} \oplus \cdots \oplus K_{A_{m-1}}$ by combining all the 1 bit secrets that she shares with each of the agents in the constellation (CubeSats) and consequently she needs $2(m-1)$ qubits to create a single bit of secret (K_M). Equivalently, she requires $m-1$ sub-protocols of efficiency $\eta_1 = \frac{1}{2}$. In brief, upper bound on η_1 of an unconditionally secure DQSS is $1/2(m-1)$. We have assumed that in the DQSS protocol proposed here one of the maximally efficient QKD or QSDC protocol proposed in is used as sub-protocols and consequently η_1 for our protocol is $1/2(m-1)$ [49]. The charactertics of the tailored protocol is listed in the Table. 1

The suggested protocol demonstrates a clear correlation between the security of the protocol and the security of the key generation system employed for communication between two communicating CubeSats. In the scenario where Alice and Bob employ the $BB84(B92)$ protocol to acquire $K_A = K_B$, the security proof of $BB84(B92)$ would guarantee the security of the current scheme. The utilization of protocols such as BB84, B92, and other single-particle based methods can be extended to incorporate dynamic quantum secret sharing.

5. Conclusion

In this research, we've paved the way for a new paradigm in CubeSat constellation networks. By integrating entanglement-based Quantum Key Distribution (QKD) into the constellation network, we've significantly enhanced its security. Our approach doesn't stop there; we've incorporated quantum repeaters and quantum memory, enabling advanced capabilities like entanglement swapping. Our focus has been comprehensive, detailing not just the theoretical underpinnings but also the practical aspects of how such a network would function, down to the hardware involved. We've tailored our proposed system for real-world use-cases, such as orbital space debris detection, showcasing its practicality. Moreover, our system is built to adapt, capable of adding or removing CubeSats without causing a problem in the existing network's overall functionality. Through meticulous evaluation, we've demonstrated that our framework isn't just theoretically sound—it's practically feasi-

Characteristics	**Value (using a maximally efficient sub-protocol of QKD or QSDC)**
Qubit efficiency η_1 (m-party DQSS Qubit efficiency	$\frac{1}{2m-2}$
η_1 (3-party DQSS	25%
Qubit efficiency (50-party DQSS) Requirement of quantum entanglement	1.02% Not required as it can be also implemented using single qubit state
Features	The system is characterized by its dynamic and hierarchical nature, allowing for implementation through several protocols such as Quantum Key Distribution (QKD), Quantum Data (QD), Quantum Key Agreement (QKA), Deterministic Secure Quantum Communication (DSQC), Quantum Secure Direct Communication (QSDC), and others. Additionally, the system enables the promotion of an agent to a higher level within the hierarchy.

Table 1: Efficiency of the proposed DQSS protocol tailored for CubeSat constellation as mentioned in [49] [48][50].

ble, efficient, and secure. Therefore, this work represents a noteworthy achievement in the advancement towards the development of safe, resilient, and adaptable CubeSat constellations.

References

[1] Wayne A Shiroma, Larry K Martin, Justin M Akagi, Jason T Akagi, Byron L Wolfe, Bryan A Fewell, and Aaron T Ohta. Cubesats: A bright future for nanosatellites. *Central European Journal of Engineering*, 1:9–15, 2011.

[2] Ram Sarup Jakhu and Joseph N Pelton. *Small satellites and their regulation*. Springer, 2014.

[3] Chantal Cappelletti and Daniel Robson. Cubesat missions and applications. In *Cubesat Handbook*, pages 53–65. Elsevier, 2021.

[4] Thyrso Villela, Cesar A Costa, Alessandra M Brandão, Fernando T Bueno, Rodrigo Leonardi, et al. Towards the thousandth cubesat: A statistical overview. *International Journal of Aerospace Engineering*, 2019, 2019.

[5] Zaid J Towfic, David Heckman, David Morabito, Ryan Rogalin, Clayton Okino, and Douglas S Abraham. Simulation and analysis of opportunistic mspa for multiple cubesat deployments. In *2018 SpaceOps Conference*, page 2396, 2018.

[6] Youngbum Song, Sang-Young Park, Geuk-Nam Kim, and Dong-Gu Kim. Design of orbit controls for a multiple cubesat mission using drift rate modulation. *Aerospace*, 8(11):323, 2021.

[7] Giancarlo Santilli, Cristian Vendittozzi, Chantal Cappelletti, Simone Battistini, and Paolo Gessini. Cubesat constellations for disaster management in remote areas. *Acta Astronautica*, 145:11–17, 2018.

[8] Pau Garcia Buzzi, Daniel Selva, Nozomi Hitomi, and William J Blackwell. Assessment of constellation designs for earth observation: Application to the tropics mission. *Acta Astronautica*, 161:166–182, 2019.

[9] Shufan Wu, Wen Chen, Caixia Cao, Chuanxin Zhang, and Zhongcheng Mu. A multiple-cubesat constellation for integrated earth observation and marine/air traffic monitoring. *Advances in Space Research*, 67(11):3712–3724, 2021.

[10] Sijing Ji, Min Sheng, Di Zhou, Weigang Bai, Qixuan Cao, and Jiandong Li. Flexible and distributed mobility management for integrated terrestrial-satellite networks: challenges, architectures, and approaches. *IEEE Network*, 35(4):73–81, 2021.

[11] Mauro De Sanctis, Ernestina Cianca, Giuseppe Araniti, Igor Bisio, and Ramjee Prasad. Satellite communications supporting internet of remote things. *IEEE Internet of Things Journal*, 3(1):113–123, 2015.

[12] Gregory Falco. Job one for space force: Space asset cybersecurity. *Belfer Center, Harvard Kennedy School, Belfer Center for Science and International Affairs, Harvard Kennedy School*, 79, 2018.

[13] KW Ingols, RW Skowyra, and MIT Lincoln Laboratory Lexington United States. Guidelines for secure small satellite design and implementation: Fy18 cyber security line-supported program. *AD1099003*, 2019.

[14] Chronis Kapalidis, Carsten Maple, Matthew Bradbury, Marie Farrell, and Michael Fisher. Cyber risk management in satellite systems. 2019.

[15] Jasminder S Sidhu, Siddarth K Joshi, Mustafa Gündoğan, Thomas Brougham, David Lowndes, Luca Mazzarella, Markus Krutzik, Sonali Mohapatra, Daniele Dequal, Giuseppe Vallone, et al. Advances in space quantum communications. *IET Quantum Communication*, 2(4):182–217, 2021.

[16] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Reviews of modern physics*, 81(2):865, 2009.

[17] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Reviews of modern physics*, 81(3):1301, 2009.

[18] Robert Bedington, Juan Miguel Arrazola, and Alexander Ling. Progress in satellite quantum key distribution. *npj Quantum Information*, 3(1):30, 2017.

[19] Robert Bedington, Xueliang Bai, Edward Truong-Cao, Yue Chuan Tan, Kadir Durak, Aitor Villar Zafra, James A Grieve, Daniel KL Oi, and Alexander Ling. Nanosatellite experiments to enable future space-based qkd missions. *EPJ Quantum Technology*, 3(1):1–10, 2016.

[20] Yu-Ao Chen, Qiang Zhang, Teng-Yun Chen, Wen-Qi Cai, Sheng-Kai Liao, Jun Zhang, Kai Chen, Juan Yin, Ji-Gang Ren, Zhu Chen, et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature*, 589(7841):214–219, 2021.

[21] Giuseppe Vallone, Vincenzo D'Ambrosio, Anna Sponselli, Sergei Slussarenko, Lorenzo Marrucci, Fabio Sciarrino, and Paolo Villoresi. Free-space quantum key distribution by rotation-invariant twisted photons. *Physical review letters*, 113(6):060503, 2014.

[22] Mateusz Polnik, Luca Mazzarella, Marilena Di Carlo, Daniel KL Oi, Annalisa Riccardi, and Ashwin Arulselvan. Scheduling of space to ground quantum key distribution. *EPJ Quantum Technology*, 7(1):3, 2020.

[23] Roland Haber, Daniel Garbe, Klaus Schilling, and Wenjamin Rosenfeld. Qube-a cubesat for quantum key distribution experiments. 2018.

[24] James A Grieve, Robert Bedington, Zhongkan Tang, Rakhitha CMRB Chandrasekara, and Alexander Ling. Spooqysats: Cubesats to demonstrate quantum key distribution technologies. *Acta Astronautica*, 151:103–106, 2018.

[25] Luca Mazzarella, Christopher Lowe, David Lowndes, Siddarth Koduru Joshi, Steve Greenland, Doug McNeil, Cassandra Mercury, Malcolm Macdonald, John Rarity, and Daniel Kuan Li Oi. Quarc: Quantum research cubesat—a constellation for quantum communication. *Cryptography*, 4(1):7, 2020.

[26] Chithrabhanu Perumangatt, Tom Vergoossen, Alexander Lohrmann, Srihari Sivasankaran, Ayesha Reezwana, Ali Anwar, Subash Sachidananda, Tanvirul Islam, and Alexander Ling. Realizing quantum nodes in space for cost-effective, global quantum communication: in-orbit results and next steps. In *Quantum Computing, Communication, and Simulation*, volume 11699, page 1169904. SPIE, 2021.

[27] Srihari Sivasankaran, Clarence Liu, Moritz Mihm, and Alexander Ling. A cubesat platform for space based quantum key distribution. In *2022 IEEE international conference on space optical systems and applications (ICSOS)*, pages 51–56. IEEE, 2022.

[28] Alexander Lohrmann, Chithrabhanu Perumangatt, Aitor Villar, and Alexander Ling. Broadband pumped polarization entangled photon-pair source in a linear beam displacement interferometer. *Applied Physics Letters*, 116(2), 2020.

[29] Yuan Lee, Eric Bersin, Axel Dahlberg, Stephanie Wehner, and Dirk Englund. A quantum router architecture for high-fidelity entanglement flows in quantum networks. *npj Quantum Information*, 8(1):75, 2022.

[30] Thomas Schildknecht. Optical surveys for space debris. *The Astronomy and Astrophysics Review*, 14:41–111, 2007.

[31] Gerard Vives Vallduriola, Diego Andrés Suárez Trujillo, Tim Helfers, Damien Daens, Jens Utzmann, Jean-Noel Pittet, and Nicolas Lièvre. The use of streak observations to detect space debris. *International journal of remote sensing*, 39(7):2066–2077, 2018.

[32] Leonard Felicetti and M Reza Emami. A multi-spacecraft formation approach to space debris surveillance. *Acta Astronautica*, 127:491–504, 2016.

[33] Abhilash Singh and Kumar Gaurav. Deep learning and data fusion to estimate surface soil moisture from multisensor satellite images. *Scientific Reports*, 13(1):2251, 2023.

[34] Vanessa Brum-Bastos, Jed Long, Katharyn Church, Greg Robson, Rogério de Paula, and Urška Demšar. Multisource data fusion of optical satellite imagery to characterize habitat selection from wildlife tracking data. *Ecological Informatics*, 60:101149, 2020.

[35] Sunita Jahirabadkar, Punam Pande, and R Aditya. A survey on image processing based techniques for space debris detection. In *2022 IEEE Bombay Section Signature Conference (IBSSC)*, pages 1–6. IEEE, 2022.

[36] Leonard Felicetti and M. Reza Emami. Image-based attitude maneuvers for space debris tracking. *Aerospace Science and Technology*, 76:58–71, 2018.

[37] Jorge Núñez, Anna Núñez, Francisco Javier Montojo, and Marta Condominas. Improving space debris detection in geo ring using image deconvolution. *Advances in Space Research*, 56(2):218–228, 2015.

[38] P Hickson. A fast algorithm for the detection of faint orbital debris tracks in optical images. *Advances in Space Research*, 62(11):3078–3085, 2018.

[39] Vincenzo Pesce, Roberto Opromolla, Salvatore Sarno, Michèle Lavagna, and Michele Grassi. Autonomous relative navigation around uncooperative spacecraft based on a single camera. *Aerospace Science and Technology*, 84:1070–1080, 2019.

[40] Arunkumar Molayath and V Sanal Kumar. Studies on space debris tracking and elimination. In *46th AIAA/ASME/SAE/ASEE Joint Propulsion Conference & Exhibit*, page 7008, 2010.

[41] CR Phipps, G Albrecht, H Friedman, D Gavel, EV George, J Murray, Chunching Ho, W Priedhorsky, MM Michaelis, and JP Reilly. Orion: Clearing near-earth space debris using a 20-kw, 530-nm, earth-based, repetitively pulsed laser. *Laser and particle beams*, 14(1):1–44, 1996.

[42] Oscar Rodriguez Fernandez, Jens Utzmann, and Urs Hugentobler. Spook-a comprehensive space surveillance and tracking analysis tool. *Acta Astronautica*, 158:178–184, 2019.

[43] Mohamed Khalil Ben-Larbi, Kattia Flores Pozo, Tom Haylok, Mirue Choi, Benjamin Grzesik, Andreas Haas, Dominik Krupke, Harald Konstanski, Volker Schaus, Sándor P Fekete, et al. Towards the automated operations of large distributed satellite systems. part 1: Review and paradigm shifts. *Advances in Space Research*, 67(11):3598–3619, 2021.

[44] Jukka Korpela. A tutorial on character code issues. *Retrieved March*, 14:2009, 2001.

[45] Kuang Tsan Lin. Digital information encrypted in an image using binary encoding. *Optics Communications*, 281(13):3447–3453, 2008.

[46] T Hwang, CC Hwang, and CW Tsai. Quantum key distribution protocol using dense coding of three-qubit w state. *The European Physical Journal D*, 61:785–790, 2011.

[47] Ci-Hong Liao, Chun-Wei Yang, and Tzonelish Hwang. Dynamic quantum secret sharing protocol based on ghz state. *Quantum information processing*, 13:1907–1916, 2014.

[48] Anindita Banerjee and Anirban Pathak. Maximally efficient protocols for direct secure quantum communication. *Physics Letters A*, 376(45):2944–2950, 2012.

[49] Chitra Shukla, Anindita Banerjee, and Anirban Pathak. Improved protocols of secure quantum communication using w states. *International Journal of theoretical physics*, 52:1914–1924, 2013.

[50] Chitra Shukla, Anirban Pathak, and R Srikanth. Beyond the goldenberg–vaidman protocol: secure and efficient quantum communication using arbitrary, orthogonal, multi-particle quantum states. *International Journal of Quantum Information*, 10(08):1241009, 2012.