

INFORMATION OF THE DOCTORAL THESIS

Thesis title: **On the study of performance improvement of free-space optical communications in continuous variable quantum key distribution system**

Specialization:	Telecommunications Engineering
Code:	9.52.02.08
Full name of PhD student:	Phan Thi Thu Hang
Training course:	2018-2021
Scientific supervisors:	<ol style="list-style-type: none">1. Assoc. Prof. Dang The Ngoc, PhD.2. Assoc. Prof. Le Hai Chau, PhD.
Training institution:	Post and Telecommunications Institute of Technology

NEW RESULTS OF THE THESIS:

The novel results of the thesis is to propose solutions to improve the performance of free-space optical communications in single-channel and multi-channel continuous variable quantum key distribution systems, ensuring the following criteria: (1) small error quantum rate ensuring the error correction on the receiver side; (2) large enough the secret key rate when considering many factors affecting transmission conditions such as atmospheric turbulence, signal loss, and interference at the receiver; ensuring the security of the system in some specific conditions when an eavesdropper appears. The new contributions of the research process shown in the thesis are as follows:

(1) Proposing a novel method of free-space optical communications for CV-QKD systems based on phase modulation

The thesis has proposed a method of quantum key distribution using Quadrature Phase Shift Keying (QPSK) at the transmitter in combination with a heterodyne detection receiver and a dual-threshold detection. Compared with previous studies, the QPSK-based quantum key distribution does not require the use of radio frequency sub-carrier modulation, resulting in a simpler system and compatible with optical communication technology.

(2) Proposing a solution to improve the performance of free-space optical communications in a continuous variable quantum key distribution system using key retransmission and relaying techniques.

This contribution can be divided into two contents as follows:

- The first is to propose a system using relaying technique based on high-altitude platform (HAP) and automatic repeat request (ARQ)-based key retransmission techniques at the relay station. These techniques have been used in conventional communication systems but have not been proposed to the FSO-QKD systems.
- The second is to build an analytical model to calculate performance metrics such as the key loss rate (KLR) and the outage probability of delay. Existing mathematical models cannot be applied in calculating the performance metrics of the proposed system because these models only use bit “0” and bit “1”. The mathematical model built in this study is used in the case of a quantum key distribution system with a discrete (4-state) input channel and the erased output channel according to the output data, “1”, “0” or “X,” after detection on the receiver side..

(3) Proposing multi-user multi-channel transmission solutions for a free-space continuous variable quantum key distribution systems

This contribution can be divided into two contents as follows:

- Firstly, the thesis proposes a multi-channel quantum key distribution system from satellites using a combination of sub-carrier multiplexing (SCM) and wavelength division multiplexing (WDM) techniques. The proposed multi-channel QKD-FSO system allows a significant improvement in the key rate compared to the single-channel QKD-FSO systems.
- Second, the thesis proposes the FSO-QKD system using the optical code division multiple access (CDMA) technique with the ability to support multiple users combined with improving the security performance of the FSO-QKD system.

APPLICATIONS, POSSIBILITY OF APPLICATION IN PRACTICE OR ISSUES THAT NEED CONTINUED RESEARCH

The research of the thesis can be considered for application in QKD systems of global scale to ensure the security of communication in current conditions. Regarding the new proposals of the thesis, it is possible to list the issues that need to be studied in the future works as follows:

(1) The performance improvement solutions proposed by the thesis can be applied in single-channel and multi-channel FSO-QKD systems based on satellites. However, in the thesis, the studies have not evaluated in detail and quantified all the threats of ke attacks from Eve as well as considered the effects and risks of insecurity caused by the signaling process at the same time. steps 3 and 4 of the QKD protocol caused. Therefore, future studies will focus on reviewing and evaluating the security level of the QKD system with attacks from Eve as well as the effects of the signaling process.

(2) In addition, in the current strong development trend of QKD systems in a global scale with the appearance of QKD networks including many QKD stations, diverse connection configuration types, providing many types of services, requiring high flexibility, it is necessary to propose a software-defined QKD network. The software-defined QKD network will allow for automating the delivery of services within an existing QKD network infrastructure, which saves service operators from deploying new services by manual intervention or having to use services provided by proprietary providers. Therefore, the study of proposals and solutions to improve performance in a software-defined QKD network will become necessary.

Scientific supervisors

PhD student

Assoc. Prof.Dr. Dang The Ngoc

Phan Thi Thu Hang

