Securing and auto-synchronizing communication over free-space optics using quantum key distribution and chaotic systems

Naveed Mahmud*[a], Esam El-Araby[a], Harry Shaw[b], Lavida Cooper[b]
[a]University of Kansas, 1520 W 15th St., Lawrence, KS 66045, USA;
[b]NASA Goddard Space Flight Center, 8800 Greenbelt Rd., Greenbelt, MD 20771, USA.

ABSTRACT

Free-Space Optical (FSO) communication provides very large bandwidth, relatively low cost, low power, low mass of implementation, and improved security when compared to conventional Free-Space Radio-Frequency (FSRF) systems. In this paper, we demonstrate a communication protocol that demonstrates improved security and longer-range FSO communication, compared to existing FSO security techniques, such as N-slit interferometers. The protocol integrates chaotic communications with Quantum Key Distribution (QKD) techniques. A Lorenz chaotic system, which is inherently secure and auto-synchronized, is utilized for secure data communications over a classical channel, while QKD is used to exchange crucial chaotic system parameters over a secure quantum channel. We also provide a concept of operations for a NASA mission combining chaotic communications and QKD operating synergistically in an end-to-end space communications link. The experimental simulation results and analysis are favorable towards our approach.

Keywords: Chaotic Communication, Quantum Key Distribution, FSO Security.

1. INTRODUCTION

Free-Space Optical (FSO) communication provides very large bandwidth and relatively low cost, low power, and low mass of implementation when compared to conventional Free-Space Radio-Frequency (FSRF) systems[1, 2, 3]. Adding security to FSO communications has usually been proposed using laser N-slit interferometers where the laser signal takes the form of an interferometric pattern such that any attempt to intercept the signal causes the collapse of the interferometric pattern[4, 5]. This technique has been demonstrated to work over propagation distances of practical interest (several kilometers)[6] for terrestrial applications and estimated to work over several thousand kilometers (2,000-10,000 km)[7, 8] for space applications. Interferometric techniques, however, assume the availability of laser technology with minimal divergence of the interferometric signals. Such limitations result in relatively short communication range for deep-space communication. Therefore, security and long-range become a trade-off for FSO communications using interferometric techniques.

In this paper, we propose a scheme which combines chaotic communications with quantum key distribution, in order to achieve more secure and synchronized FSO communication. Chaotic communication systems offer several features that make them suitable for secure communications. They display well defined but complex dynamic behaviors[9] and characteristics such as broadband noise-like signals, unpredictability, and sensitivity to initial conditions[9]. These characteristics make it difficult for eavesdroppers to synchronize to the chaotic signal. Chaotic systems are unstable, nonlinear and aperiodic in nature, but they offer a wideband signal, which can be thought of as spread spectrum, with multi-path fading resistance[10, 11]. Additionally, chaotic systems are compatible with simpler formats/models such as On-Off Keying (OOK) as well as M-ary pulse position modulation (PPM) schemes which are more compatible with deep space optical communications.

Chaotic systems maintain synchronization by means of sharing a common set of parameters between transmitter and receiver. Before initiating chaotic data transmission, these synchronization parameters must be communicated with the receiver through a highly secure channel. In our scheme, we propose using Quantum Key Distribution (QKD) to share the chaotic synchronization parameters via a quantum channel. For secure key sharing, public-key cryptosystems generally use Rivest-Shamir-Adleman (RSA) algorithm[12], which is based on the assumption that factorization of large integers is computationally impractical. However, with emergence of quantum computers[13, 14], this assumption might not hold out to be true in the near future. Recent works[15, 16] have demonstrated implementations of Shor's algorithm[17] to factorize large integers efficiently using a quantum computer. In the near future, a more powerful and accurate quantum computer would be able to break the RSA algorithm and compromise security of public-key systems. QKD, on the other hand, cannot be

compromised as any interception of the shared key destroys the data contained in it, thereby alerting the presence of an unintentional receiver. The unconditional security of QKD has been demonstrated in many previous works[18, 19, 20].

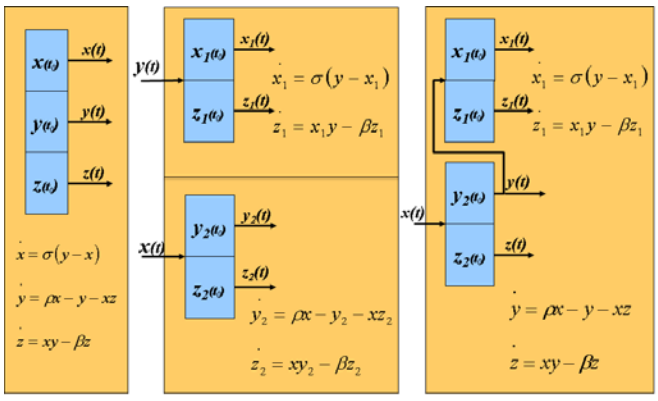
We propose to design transmitter and receiver models that are based on synchronous chaotic systems for use in FSO communications targeting both space and terrestrial applications. A key exchange model is integrated with the models for securely exchanging the chaotic synchronization parameters between the transmitter and receiver via a quantum and/or classical channel. A realistic classical channel with Additive White Gaussian Noise (AWGN) is modeled for data communication. Low-density-parity-check (LDPC) and digital modulation/demodulation techniques such as Quadrature-Phase-Shift-Keying (QPSK) are also implemented in the transmitter and receiver to minimize noise and improve bit-error-rate (BER) of the transmitted information. For experimental analysis we send images encoded as binary non-return-to-zero (NRZ) data across the FSO channel and recover them at the receiver end. The proposed communications scheme can be used to secure optical communications downlink, which contains science data, as well as securing optical communications uplink, which may contain spacecraft and instrument commands. Thus, future FSO space communications utilizing the outcome of the proposed work will allow for secure communications at distances from Mars to the outer planets and Kuiper belt (1.5 to 40 AU). Missions such as the Ice Giants Decadal Survey mission[21] would benefit from this technology.

The rest of the paper is organized such that Section 2 presents background information and related work. Section 3 describes the proposed communication scheme in detail. In Section 4 we provide a concept of operations for a practical NASA mission. The experimental work and analysis is presented in Section 5. Finally, Section 6 ends the paper with conclusions and future work.

2. BACKGROUND AND RELATED WORK

Chaotic Communications

Our approach leverages previous work and concepts that were introduced particularly for chaotic synchronization and communication[10, 22, 23, 24]. Generally, in conventional communication systems, a periodic carrier introduced in the transmitter carries the modulating data message (AM, FM, ASK, FSK, etc.), where the receiver recovers the message by means of tuning to this carrier frequency. Chaotic communications schemes generalize this principle by utilizing a chaotic carrier, which, similarly to a spread-spectrum approach, offers a broad frequency spectrum used in carrying the data signal from the transmitter. For successful transmission recovery in chaotic systems, synchronization between the transmitter and receiver is essential. The control and synchronization of chaotic systems have been studied over the past two decades[22, 23, 24] for potential applications in secure communication[10]. The fundamental aperiodic nature of the chaotic carrier signal does not allow it to be stored in the receiver as a reference signal, which is detrimental for coherent detection of the transmitted signal. Pecora and Carroll in 1990 reported that certain chaotic systems possess a self-synchronization property[22]. They proved that a chaotic system is self-synchronizing if it can be decomposed into stable response subsystems. The stable response subsystems when driven by a common signal from the original (drive) system can then operate in auto synchrony with the drive system[22, 23, 24]. For example, they showed that the Lorenz chaotic system[9], usually called Lorenz attractor, is decomposable into two separate stable response subsystems that will each synchronize to the drive system when started from any initial condition[25, 26], as shown in Figure 1.



(a) Drive system (b) Decomposable stable response subsystems (c) Lorenz attractor proposed for comms.

Figure 1: Lorenz attractor and its decomposable stable response subsystems for use in communications.

Cuomo and Oppenheim[25, 26], based on Pecora and Carroll's findings[22, 23, 24], proposed chaos synchronization as a means for communication. In one of their discussed approaches, chaotic signal masking, the noise-like chaotic signal, *x(t)* generated at the transmitter is added to the input data signal, *d(t)*, and then transmitted over the communication channel. For signal masking, it is assumed that the power level of the input data signal is significantly lower than that of *x(t)*. For this technique, regenerating the chaotic carrier at the receiver end[25, 26], is essential for synchronization. The error between the received signal and the regenerated carrier, could then be used for recovering the original data signal, *d(t)*.

Quantum Key Distribution

Compared to conventional cryptography systems, Quantum Key Distribution (QKD) is a far more secure scheme[18, 19, 20] as the information integrity is dependent on properties of quantum mechanics, rather than on computational difficulty of the cryptographic algorithm. It works by enabling two participants to share a secret key securely and without any information divulged to any eavesdropper. Once the key is shared and known to both parties, the transmitting side can start encrypting messages with the shared key and broadcasting them, while the receiving party decrypts the message with the key known only to them. The distinguishing and critical property of QKD is that the key is encoded as conjugate bases of a quantum state (or qubits) and transmitted over a quantum channel[19]. According to fundamentals of quantum mechanics, it is impossible to measure a quantum state simultaneously in two orthonormal basis[19]. Thus any attempt to intercept the quantum channel and measure a qubit destroys its quantum state and a random outcome is observed by the interceptor. The destroyed qubit also indicates to the receiver that an interception was attempted. These characteristics make QKD a highly secure scheme for sharing key information.

The first secure QKD protocol[27] was introduced by Bennet and Brassard in 1984 and named BB84 after them. Photon polarization states were used to transmit key information through a quantum channel in combination with an insecure public channel. The key information is encoded as non-orthogonal quantum states, which are polarization directions of 0, 45, 90 and 135 degrees in the case of photons. An example of how the protocol works is discussed as follows. The transmitter 'Alice' encodes each bit on one of two polarization bases (Rectilinear R, or Diagonal D) and uses either pair of polarization states/directions (0, 90) or (45, 135) to encode each bit. The receiver 'Bob' can use either one of the two polarization bases to measure the received photon and recover the bit, hence Bob has a 50% chance to recover the correct bits. After all photons are measured by Bob, both Alice and Bob communicate over a public channel, with Alice sending the basis of each photon she had sent and Bob sending the basis of all of his measurements. They eliminate the measurement bits whose basis did not match and create a key with the remaining number of bits. To detect the presence of an eavesdropper, Bob and Alice can agree upon a pre-shared subset of the key bits, e.g., one third, and match that with their measured bits. If no errors are detected then they commence encryption of their data with the shared key and can securely transmit over the classical channel. Figure 2 illustrates the above BB84 protocol example.

QUANTUM TRANSMISSION												
1. Alice prepares string of bits for transmission	1	0	0	1	0	0	1	1	0	1	0	0
2. Alice encodes each bit with random basis	D	R	D	R	R	R	R	R	D	D	R	D
3. Alice prepares photon polarization state/direction	135	90	45	0	90	90	0	0	45	135	90	45
4. Bob measures photon with random basis	R	D	D	R	R	D	D	R	D	R	D	D
5. Bits recovered by Bob (using random direction)	1	0	0	1	0	0	0	1	0	1	1	0
PUBLIC DISCUSSION OF BASIS												
6. Bob sends measurement basis	R	D	D	R	R	D	D	R	D	R	D	D
7. Alice acknowledges correct bases			OK	OK	OK			OK	OK			OK
8. Shared information			0	1	0			1	0			0
9. Bob sends random key bits			0					1				
10. Alice confirms random key bits			OK					OK				
OUTCOME												
11. Secret key formed from remaining bits				1	0				0			0

Basis	0	1
R	90	0
D	45	135

Figure 2: BB84 protocol using two non-orthogonal bases and four polarization directions.

Related Work

More work on chaotic communication[28, 29, 30, 31] have been reported since its introduction by Cuomo and Oppenheim[25, 26]. Despite the potential use of chaos in secure communications, there are known limitations when applied in a real system. The major problem in designing chaos-based secure communication systems can be stated as how to send an encrypted message from the transmitter (drive system) to the receiver (response system) over a public channel while achieving security, maintaining privacy, and providing good noise rejection[31]. Specifically, small parameter mismatches and noise may bring about irreversible synchronization errors due to large distortions present in the synchronization manifold, known as attractor bubbling[32]. Moreover, bit-error-ratio (BER) of the synchronized chaos communication may be higher than alternative secure communication approaches. This is because chaotic systems continuously generate non-redundant information and have a positive Kolmogorov-Sinai entropy[31]. Overcoming these limitations should be achieved, in

practice, using either analog or digital hardware[31] in a robust form that can achieve, to some degree, perfect reconstruction of the transmitted signal at the receiver end. Several attempts were made to robustify the design of chaos-based secure communication systems and many techniques were developed[28, 31]. Similar research work investigating the combination of chaotic systems with FSO communication has been demonstrated[33]. For example, Annovazzi-Lodi et al.[33] proposed an optical configuration of semiconductor lasers which are injected with a third driving signal to gain chaotic synchronization. This methodology and hardware setup has some limitations that were avoided in our proposed work. In their work, the lasers were configured based on the Lang Kobayashi model[34] which is not inherently auto-synchronizable, and hence the need for external injection from a third laser. The external laser used optical reflectors to create the synchronizing signal which is impractical or infeasible in a long-distance communication system. Our proposed work based on the auto-synchronizing Lorenz model eliminates the need for such an extra costly hardware.

There have been several notable demonstrations of QKD in FSO communications. Marcikic et al.[35] demonstrate a QKD system utilizing polarization entangled photon pairs. Schmitt-Manderbach et al.[36] present an experimental evaluation of the BB84 protocol over a 144 km FSO link using weak coherent lasers. Hughes et al.[37] demonstrate a similar implementation of BB84 over a 10 km FSO channel in both day and nighttime. These implementation efforts of the BB84 protocol, however, do not offer any improved security for longer-range FSO terrestrial communication. In our work, we present a highly secure communication scheme that provides improved and auto-synchronized FSO chaotic communications by combining QKD with chaotic systems. We also provide a practical concept of operations for an FSO mission where the proposed scheme can be applied. While QKD is used to secure key distribution, additional security is provided by the chaotic Lorenz models in the classical communication channel to protect the data from intruding attacks. The use of chaotic signal masking in data transmission also eliminates the cost of employing computationally intensive encryption/decryption techniques and reduces hardware complexity and cost. To the best of our knowledge, this work is the first effort to use chaotic communication techniques integrated with QKD for securing digital FSO communications.

3. PROPOSED CHAOTIC COMMUNICATION WITH QUANTUM KEY DISTRIBUTION

Figure 3 shows our proposed system for chaotic communications with QKD. The flow of operations is as follows. On the transmitter (TX) side, the QKD TX model starts its operation by exchanging the chaotic synchronization parameters with the receiver module (RX), in a two-way BB84-like protocol via both classical and quantum channels. On the receiver side, see Figure 3, the QKD RX model recovers the chaotic parameters and provides them to the synchronizable Lorenz chaotic receiver. Once parameter exchange is complete, data transmission is started from the transmitter side. The input message data d_t is converted to a binary non-return-to-zero (NRZ) format m_t. The Lorenz transmitter, generates the noise-like chaotic signal x_t which is added with the message data to form the transmission signal S_t which is then converted to pure binary format B_t consisting of 1s and 0s. The binary data, which constitutes the chaotically masked message, is given to a Low-density-parity-check (LDPC) module which performs forward error correction by adding redundancy to the data. The encoded signal C_t undergoes Quadrature-Phase-Shift-Keying (QPSK) digital modulation before being broadcast on the Additive White Gaussian Noise (AWGN) communication channel in complex form Q_t. On the receiver side, see Figure 3, the received complex signal undergoes QPSK demodulation, LDPC decoding and binary to real conversion. The converted signal S_r is given as the driving signal to the Lorenz receiver, which already has the synchronization parameters from the QKD RX model, and is able to regenerate a chaotic signal x_r similar to the one at the Lorenz TX. This regenerated signal is used for recovering the message data m_r. The recovered message, which is an NRZ data, is converted to its original format by an NRZ decoder. In the next sections, the operations of the Lorenz TX, RX and the QKD parameter exchange models are discussed in detail.

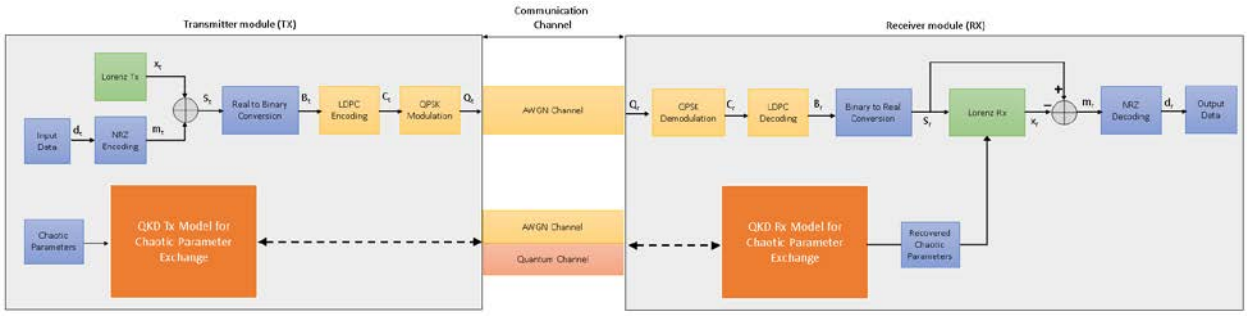


Figure 3: Transmitter and receiver modules for chaotic communication scheme with QKD.

3.1 Chaotic Transmitter and Receiver

In designing Lorenz attractor for both the transmitter and the receiver, we leverage Cuomo and Oppenheim's work[25, 26]. As it can be seen in Figure 3, the input data signal $d_t(t)$ is masked with the generated chaotic state signals $x_t(t)$ to obtain the transmitted signal $S_t(t) = x_t(t) + d_t(t)$. At the receiver end, the chaotic carrier[25, 26] $x_r(t)$ is regenerated using the received signal $S_r(t)$ and the same system parameters of the transmitter, σ, ρ, β, and initial conditions $x(0)$, $y(0)$ and $z(0)$, which are essential for synchronization. The error signal $m_r(t)$ which is the difference between the received signal $S_r(t)$ and the regenerated carrier $x_r(t)$ is then used for reconstructing the original data $d_r(t)$, see Figure 3. In designing the simulation models for the transmitter and the receiver, we discretized the differential equations (1) and (2) using Euler, 1st order Runge–Kutta (RK), approximation. Higher order RK were also used but with insignificant improvement in accuracy, hence 1st order RK approximation was chosen for its simpler implementation and lower hardware cost.

$$\left.\begin{aligned} \dot{x}_t &= \sigma(y_t - x_t) \\ \dot{y}_t &= \rho x_t - y_t - x_t z_t \\ \dot{z}_t &= x_t y_t - \beta z_t \end{aligned}\right\} \begin{array}{l}\text{Lorenz Chaotic Transmitter} \\ \text{where } d(t) \text{ is the input data signal} \\ \text{and } x_t(t) \text{ is the carrier signal}\end{array} \qquad (1)$$

$$and\ ,\ s_t(t) = x_t(t) + d(t)$$

$$\left.\begin{aligned} \dot{x}_r &= \sigma(y_r - x_r) \\ \dot{y}_r &= \rho s - y_r - s_r z_r \\ \dot{z}_r &= s y_r - \beta z_r \end{aligned}\right\} \begin{array}{l}\text{Synchronized Lorenz Chaotic Receiver} \\ \text{where } s_r(t) \text{ is the received signal and} \\ x_r(t) \text{ is the regenerated carrier signal}\end{array} \qquad (2)$$

We also implemented signal masking of the data signal with the chaotic carrier signal as simply $S_t(t) = d_t(t) + x_t(t)$. Figure 4, illustrates the digital models derived from RK approximation of (1) and (2). For modeling, we discretize the time domain as $t = n.\Delta t = n.h$, where n is the discrete time (sample) index, and h is the sample time step or the reciprocal of the sampling frequency $f_{sampling}$.

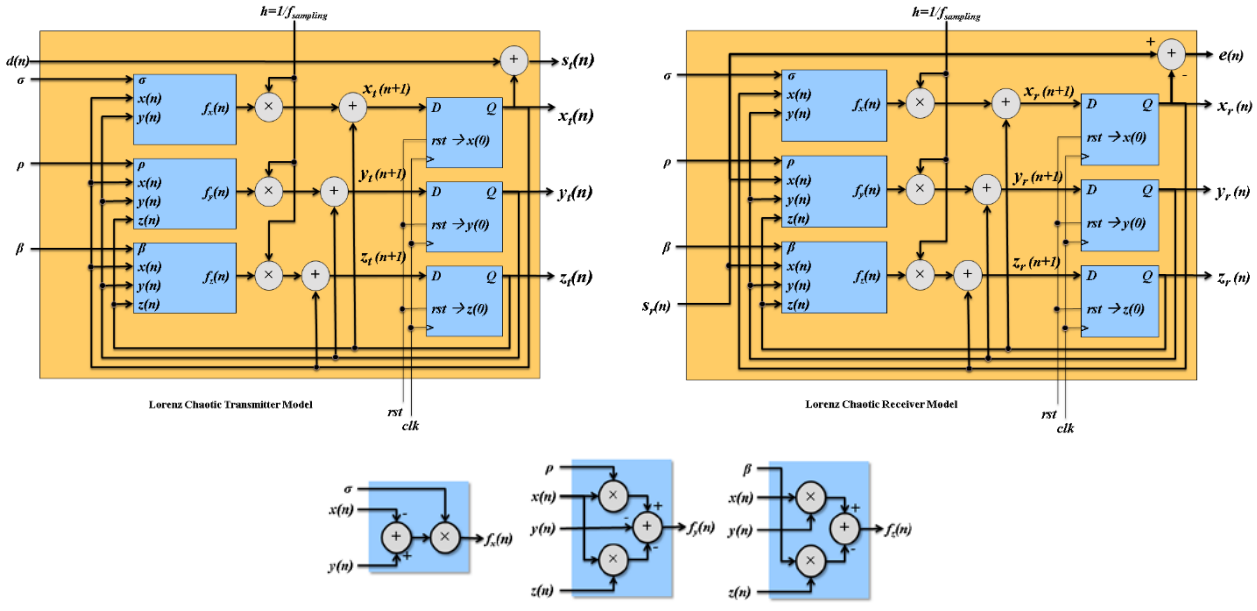


Figure 4: Chaotic transmitter and receiver models in the proposed communication scheme.

3.2 Quantum Key Distribution model for chaotic parameter exchange

The QKD model is responsible for establishing the FSO chaotic communications link with exchange of the set of synchronization parameters, $\mathbb{Z}$ where

$$\mathbb{Z} = \{\sigma, \rho, \beta, x(0), y(0), z(0)\} \tag{3}$$

The synchronization parameters are signed real numbers. A transmitter (Alice) and receiver (Bob) will exchange the parameters using quantum communications mapped from the signed real numbers. Given

$$\psi = p_0|0\rangle + p_1|1\rangle \tag{4}$$

such that the binary representation of $\mathbb{Z}$ can be mapped to either basis/symbol state where, p_i represents the probability of each symbol, and ψ_i is the basis set with a total probability p given by:

$$p = \sum_i p_i = 1 \tag{5}$$

and probability density function ρ' given by

$$\rho' = \sum_i p_i|\psi_i\rangle\langle\psi_i| \tag{6}$$

Alice and Bob utilize a quantum communications model that is agnostic to the quantum basis and mode of quantum communication. The quantum codebook is created from a user specified basis set ψ. The user can specify pure states, mixed states or a combination of pure and mixed states. The basis set operates upon a positive semi-definite matrix created from the user-provided chaotic parameters. For the minimum basis set, the set of synchronization parameters are transformed into a set of matrices $A = \{A_0, A_1, A_2\}$ such that

$$A_0 = \begin{bmatrix} \sigma & 0 \\ 0 & \rho \end{bmatrix},\ A_1 = \begin{bmatrix} \beta & 0 \\ 0 & x(0) \end{bmatrix}, A_2 = \begin{bmatrix} y(0) & 0 \\ 0 & z(0) \end{bmatrix}$$

Alice and Bob will use the RSA algorithm to generate a key pair of a private key and a shared public key, details of the function of the RSA algorithm can be found here[12]. Alice and Bob possess a public encryption key *{e, n}* and a private decryption key *{d, n}* with a common factor *n*. For any integer message *M*, where $M < n$ and *M* is an integer representation of each non-zero entry in matrix set A, Alice generates encrypted message *C* using the public key *{e, n}* as described in (7) and Bob decrypts *C* back to *M* using the private key *{d, n}* as described in (8).

$$C = M^e * mod(n) \tag{7}$$

$$M = C^d * mod(n) \tag{8}$$

Pre-shared secrets between Alice and Bob

Alice and Bob have pre-established RSA key pairs, *{e, n}* and *{d, n}*, as well as a protocol for establishing new pairs. Alice and Bob share the knowledge of the quantum basis. Presumably, Alice and Bob are using identical hardware and software for the coding and decoding of qubits. The physical implementation that Alice and Bob are using drives the quantum coding basis. The lowest level of security is afforded with the simplest basis selection. The higher the order of quantum basis, the less effective brute force eavesdropping or sequence analysis will become. Let Alice and Bob share a set of secret symbol probabilities *S*, as given in (9), for building a second codebook. Derived from this set of probabilities, the second codebook is a binary Huffman dictionary of variable length codewords *H* as defined in (10).

$$S = \{s_0, s_1, \dots, s_n\} \tag{9}$$

$$H = \{W_0, W_1, \dots, W_n\} \tag{10}$$

The number of bits in each word *W*, is determined by the probabilities in *S*. Combinations of W are formed to develop the encryption protocol as shown in Figure 5.

Huffman codewords

In the simplest implementation, only two Qubit codeword possibilities exist. Consequently, a brute force attack on the quantum exchanges will lead to approximately 50% of the qubits being correctly identified by Eve. Furthermore, Eve can apply sequence analysis and determine that there are only two quantum codewords, and determine the frequency of appearance of each codeword. Alice, however, has coded the classical bits into another codeword dictionary and selection of the codewords from that dictionary is determined by encrypted matches of the qubit exchange, see Figure 5. Therefore, a limiting factor in a successful Man-In-The-Middle (MITM) impersonation attack is codeword recovery. This approach has the following advantages:

1) The synchronization parameters are exchanged twice. The first exchange helps establish the quantum keys and the second exchange sends the encrypted parameters as quantum bits.
2) Eve, reading the first transmission of qubits has no more idea than Bob on how to interpret the qubits. Unless Eve can fully impersonate Bob, the forward information from Alice is meaningless.
3) Alice and Bob can compare the two exchanges of qubits for information about the quality of the quantum link and the potential existence of an eavesdropper.

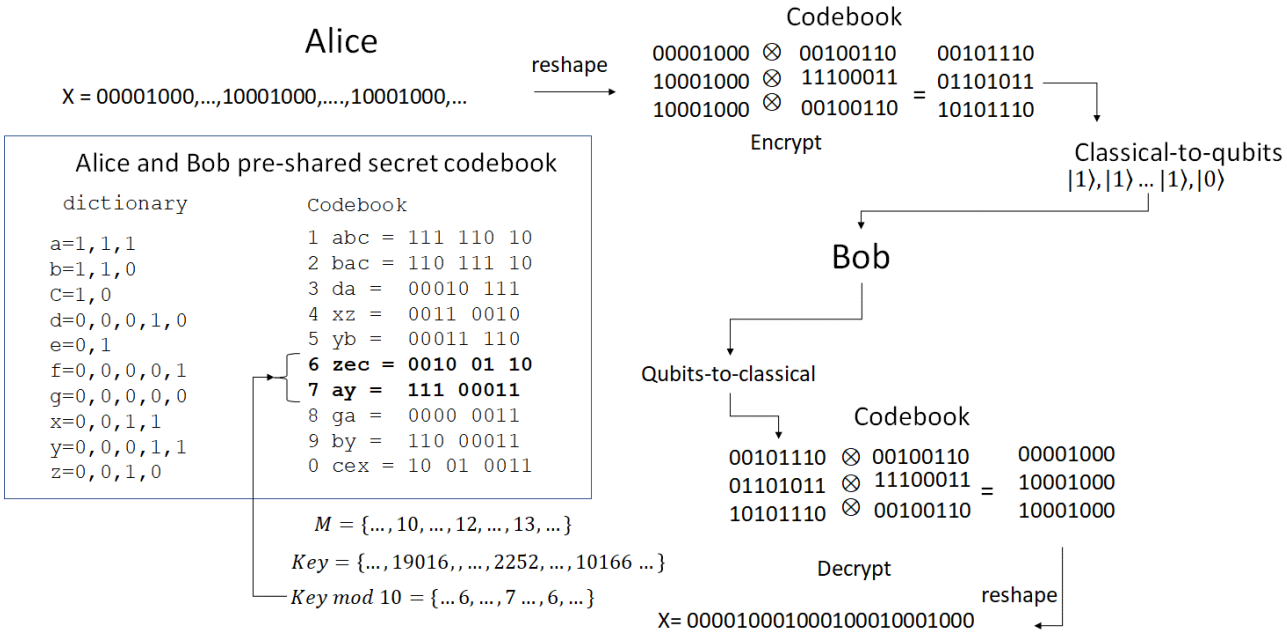


Figure 5. Use of pre-shared secret codebook for encrypting/decrypting the synchronization data. The position of the codewords is assumed to have been randomized by Alice and de-randomized by Bob.

Assuming a 24-bit sequence within Alice's synchronization parameters denoted as *X*, we have previously established the generation of *M* from the Alice-Bob matches of the qubit basis. We have also established how Alice uses the RSA algorithm on *M* to generate the *Key*. The *Key* holds the encrypted positions of the matches represented by *M*. Alice and Bob have previously used the pre-shared symbol probabilities *S*, to generate the Huffman dictionary *H*, as shown in Figure 5. In this example, the 24-bit sequence *X* is decomposed into three 8-bit words. Therefore, the valid combinations of codewords are concatenated codewords of length 8-bits, and the XOR encryption operation is performed on 8-bit words. In this example, the valid symbols are: $\{a, b, c, d, e, f, x, y, z\}$ and the valid codeword combinations are: $\{abc, bac, da, xz, yb, zec, ay, ga, by, cex\}$. Given *m* valid codewords in *H*, Alice and Bob use *Key mod m* to select the 8-bit codewords for the XOR encryption operation.

Alice and Bob are free to setup this approach with as many codewords as necessary in *H*, and establish the Hamming distance between each code. Alice and Bob determine the length of *X* and its decomposition into words of arbitrary length as desired, not necessarily 8-bits in length.

Parameter exchange protocol

The proposed protocol for chaotic synchronization parameter exchange along with the corresponding Tx/Rx models are shown in Figure 6. In step 1, Alice encodes the synchronization parameters into classical binary format, translates to qubits, and then transmits them to Bob using the agreed upon basis. Bob has the basis with no knowledge of the order of qubit coding. Bob randomly measures the qubits and transmits the results back to Alice. In step 2, Alice receives and compares Bob's results, encrypts the matches (M) to form the quantum encryption key (*Key*), see Figures 5 and 6. In step 3, Alice sends the *Key* to Bob. In step 4, Alice encrypts the synchronization parameters using the *Key* and the pre-shared Huffman dictionary codewords (*H*) described in (10), translates, and transmits the associated qubits to Bob. Bob then decodes the qubits using his pre-shared Huffman dictionary and the *Key*. The detailed operation of step 4 was shown in Figure 5.

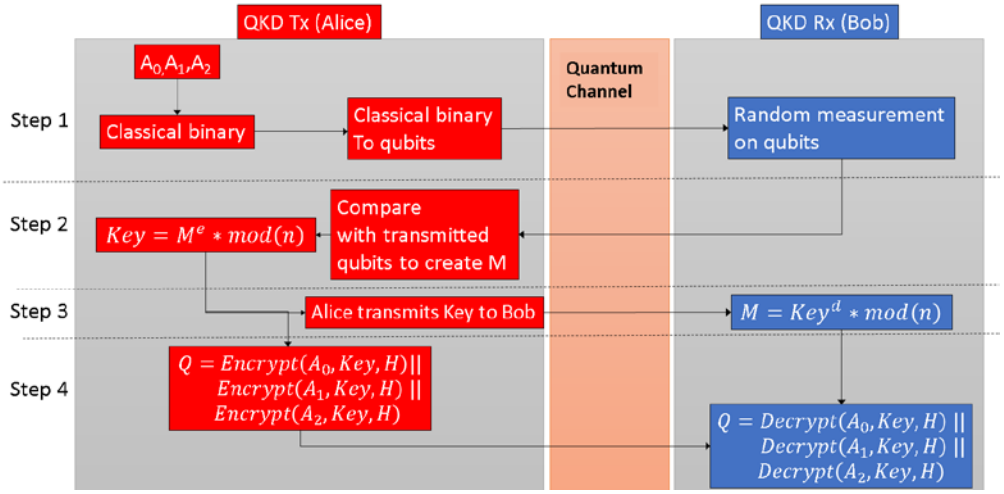


Figure 6: Quantum Key Distribution models for chaotic parameter exchange.

4. CONCEPT OF OPERATIONS FOR NASA MISSION

Figure 7 depicts an orbital configuration in which AliceSat and BobSat intend to exchange data via a space-to-space optical communications link using the proposed chaotic communication scheme with QKD parameter exchange. At approximately earth-lunar distances of about 400,000 km, 10 cm optics at 1550 nm transmit wavelength (similar to the Lunar Laser Communications Demonstration - LLCD[38]), the beamwidth is approximately 6 km diameter at that distance. Therefore, the eavesdropper, EveSat, will attempt to be within that area to have a line-of-sight (LOS) with good link characteristics for impersonating BobSat as shown in Figure 7. As a point of comparison, the GRACE spacecraft tandem which performed earth gravity mapping, flew 220 km apart from each other[39].

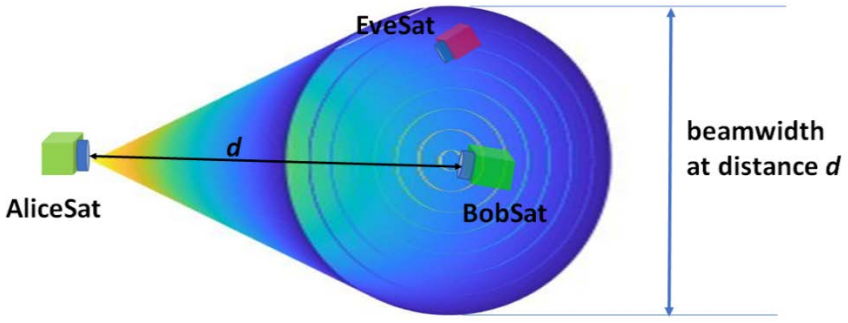


Figure 7. AliceSat, BobSat, and EveSat orbital configuration with the AliceSat transmitting beam in the direction of BobSat. It is assumed that AliceSat and BobSat are boresight aligned. EveSat is within the AliceSat transmit beam but undetected by AliceSat, BobSat, or Earth Optical Ground Stations.

Given that this is a space application, the most likely attacks are blinding attacks in which EveSat attempts to disable AliceSat and BobSat, and Impersonation attacks such as Man-In-the-Middle (MITM) attacks. Blinding attacks are beyond the scope of this paper while are focus is towards MITM attacks. Specifically, the goal of EveSat's MITM attack is to intercept and decode the data being exchanged between AliceSat and BobSat without being identified.

Pre-launch security requirements

AliceSat and BobSat must have establish their sets of pre-shared secrets and a strong authentication protocol to minimize the probability of the MITM attack success. AliceSat and BobSat are using RSA encryption, therefore they will establish their private and public keys as previously described. AliceSat and BobSat also share a classical Huffman dictionary of binary codewords. These codewords will map to encrypted key parameters.

Depending upon the space-to-space orbital drivers (two free-flying independent spacecraft, orbiter-to-relay, etc.), AliceSat and BobSat will establish a series of authentication and key exchange procedures. Once authenticated, AliceSat and BobSat can utilize the quantum communications channel for all forms of data exchange. AliceSat and BobSat can use the initial quantum key exchange protocol for re-keying.

Strength of the link security

A number of factors contribute to the link security:

1) Required proximity of EveSat to either BobSat or AliceSat.
2) The nature of the known orbital dynamics between BobSat and AliceSat.
3) The inherent spread spectrum nature of chaotic communications.
4) The quantum coding of the synchronization parameters, to address the weak link of sending the synchronization parameters as cleartext.
5) The RSA encryption of the key parameters reconciling the correct matches of BobSat and AliceSat quantum basis.

On a two-qubit scheme that is applicable to BB84-like key distribution, security is enhanced through maximizing randomization of the inputs[40]. Security can also be improved by increasing the orders of complexity of the quantum basis, provided that the eavesdropper cannot use knowledge of one state to derive knowledge of the remaining states[40]. This is at the cost of additional hardware and software complexity. EveSat can mount a sophisticated attack on the basic binary coding schemes, and analyze the distribution of measurement responses when she applies her quantum basis. The countermeasure is to increase the modularity of quantum basis and the complexity of the encryption protocols within the constraints of the budget and schedule. However, the basic security scheme shown in this paper, combined with the constraints on the eavesdropper to attack this space-to-space free space optical link would be useful if installed in a NIST-moderate security environment and easily extensible to NIST-high security environment[41].

5. EXPERIMENTAL RESULTS

The performance of the proposed communication scheme is evaluated through our experimental work described in this section. Accuracy of quantum key and chaotic parameter exchange was tested where real-time data transmission and recovery across an AWGN channel model was carried out using images as the test input data. The noise tolerance of the system was investigated by measuring the transmission bit error rate (BER) for varying values of channel SNR. The quality of the reconstructed image was also evaluated by measuring the percentage error in pixels between the original and the reconstructed image. MATLAB version 2017A was used for design and simulation purposes.

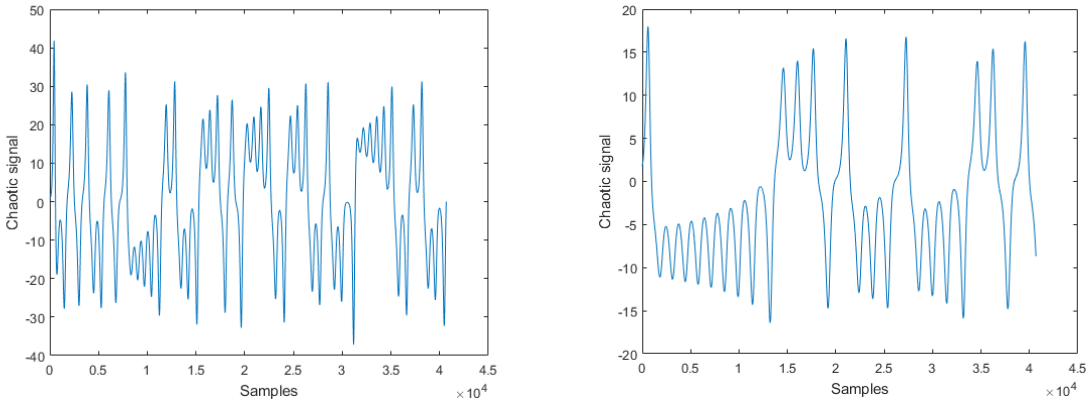
Image Transmission

The system was tested for image transmission using different sets of chaotic parameters. Table 1 shows two sets of chaotic synchronization parameters that are typically used for chaotic systems. The experimental results showed that the QKD model was able to exchange the chaotic parameters with 100% accuracy.

Table 1. Two sets of Lorenz chaotic parameters.

Config.	Sigma	Rho	Beta	X(0)	Y(0)	Z(0)	Parameters successfully recovered at receiver
A	16.0	64.0	4.0	1.0	0	0	Yes
B	10.0	28.0	2.677	1.77	2.89	4.56	Yes

With the Lorenz TX and RX configured with different sets of parameters, the attractors generated different forms of random, noise-like chaotic signal. This is demonstrated in Figure 8 for each of the configurations in Table 1. A sampling frequency of 2 KHz was used by the Lorenz TX and RX.



Configuration A **Configuration B**

Figure 8: Chaotic signals generated by synchronized Lorenz Attractor TX and RX for different configurations.

With a fixed configuration, the channel noise was varied from SNR range of 0 dB to 40 dB to evaluate the noise tolerance of the system. The BER as a function of SNR obtained from these experiments is shown in Figure 9. The experimental results show that the system can reject channel noise for a wide range of SNR (> 0.8 dB). Accurate recovery of the data was possible even for very low SNR, e.g., 0.1 dB.

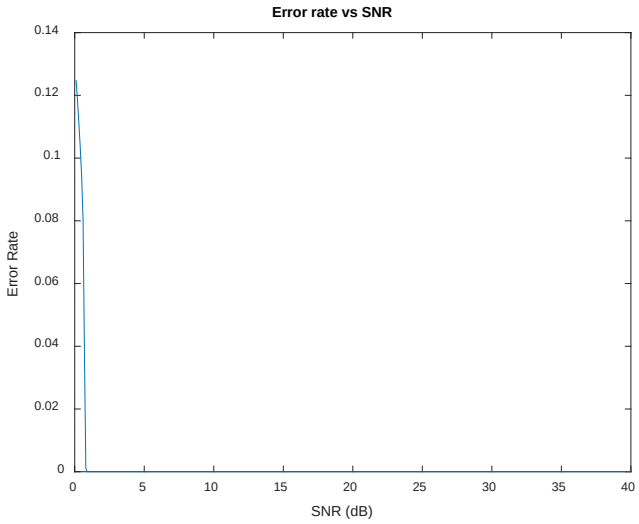


Figure 9: Bit Error Rate (BER) as a function of Signal-to-Noise-Ratio (SNR).

An image transmitted by AliceSat and reconstructed at BobSat for SNR 0.1 dB is shown in Figure 10. Results show a 0% error in pixels between the original and reconstructed image. Also shown is a third image reconstructed by an unintentional intercepting RX, EveSat. We assume that EveSat has knowledge of the communication scheme we are using and is able to perform techniques such as LDPC decoding, QPSK demodulation, NRZ decoding, etc. to reconstruct the image data. However, to successfully intercept any data from this scheme EveSat has to know the chaotic parameters shared by AliceSat and BobSat, and due to the high security provided by QKD, EveSat has no way of acquiring those parameters. Thus, EveSat proceeds with a randomly configured/synchronized Lorenz RX to try and capture the transmitted signal and regenerate the message. Results prove that EveSat cannot obtain synchronization parameters from the quantum channel and synchronize with the chaotic transmitter, thus it cannot obtain any useful data from the intercepted signal.

Synchronization Parameters
$\sigma = 16, \rho = 64, \beta = 4, x(0) = 1, y(0) = 0,$ and $z(0) = 0$

10-a) Original image transmitted by Alice.

Synchronization Parameters
$\sigma = 16, \rho = 64, \beta = 4, x(0) = 1, y(0) = 0,$ and $z(0) = 0$
SNR = 0.1 dB, Pixel Error = 0 %

10-b) Reconstructed image by Bob using recovered synchronization parameters.

Synchronization Parameters
$\sigma = 10, \rho = 45.6, \beta = 14, x(0) = 0, y(0) = 0,$ and $z(0) = 0$
SNR = 0.1 dB, Pixel Error = 98.3084 %

10-c) Reconstructed image by Eve using incorrect synchronization parameters.

Figure 10: Results of image transmission between Alice and Bob, with interception by Eve.

6. CONCLUSIONS AND FUTURE WORK

In this paper, we demonstrated a secure and synchronizable scheme for free-space optical (FSO) communication by combining chaotic communication using Lorenz attractor and quantum key distribution (QKD) protocol. The scheme is evaluated by simulation results, which show that the system is noise tolerant and feasible for FSO communications. The results also show that the scheme is secured by the use of chaotic signals, which are highly random/unpredictable due to their high sensitivity to the system parameters and initial conditions. Results also show that secure sharing of chaotic

parameters between the transmitter and the receiver via QKD is feasible and increases efficiency and security of this scheme. Future work will include hardware implementations and interfacing with free-space optics.

REFERENCES

[1] Edwards, B. L., Israel D., Wilson K., Moores J. and Fletcher A., "Overview of the Laser Communications Relay Demonstration Project," in Proceedings of the 12th International Conference on Space Operations, SpaceOps 1261897, (2012).

[2] Mohon, L., "Laser Communications Relay Demonstration (LCRD) Project," NASA-GSFC, March 30, 2018, <www.nasa.gov/mission_pages/tdm/lcrd/ > (15 July 2018).

[3] "NASA laser communications mission passes major review milestone," NASA-GSFC, 18 Sept. 2012, <https://www.nasa.gov/centers/goddard/news/releases/2012/12-074.html > (15 July 2018).

[4] Duarte, F. J., "Secure interferometric communications in free space," Optics Communications 205(4-6), 313–319 (2002).

[5] Duarte, F. J., "Secure interferometric communications in free space: enhanced sensitivity for propagation in the metre range," Journal of Optics A: Pure and Applied Optics 7(1), (2005).

[6] Duarte, F. J., Taylor, T. S., Black, A. M., Davenport, W. E. and Varmette, P. G., "N-slit interferometer for secure free-space optical communications: 527 m intra interferometric path length," Journal of Optics 13(3), 5 (2011).

[7] Duarte, F. J. and Taylor, T. S., "Quantum entanglement physics secures space-to-space interferometric communications," Laser Focus World 51(4), 54-58 (2015).

[8] Boroson, D. M., "Optical Communications: A Compendium of Signal Formats, Receiver Architectures, Analysis Mathematics, and Performance Characteristics," Lincoln Laboratory, Massachusetts Institute of Technology, 9 Sept. 2005 <http://www.dtic.mil/docs/citations/ADA439968 > (15 July 2018).

[9] Lorenz, E. N., "Deterministic Nonperiodic Flow," Journal of the Atmospheric Sciences 20, (2), 130-141 (1963).

[10] Riaz, A. and Ali, M., "Chaotic communications, their applications and advantages over traditional methods of communication," in Proceedings of IEEE 6th International Symposium on Communication Systems, Networks and Digital Signal Processing, 21-24 (2008).

[11] Oğraş, H. and Türk, M., "Performing Modulation Scheme of Chaos Shift Keying with Hyperchaotic Chen System," Proceedings of the 6th International Advanced Technologies Symposium (IATS'11) 4, 54-58 (2011).

[12] Stallings, W., [Cryptography and Network Security: Principles and Practice (6th ed.)], Prentice Hall Press, Upper Saddle River, NJ, USA, (2013).

[13] Amin, M. H., Dickson, N. G. and Smith, P., "Adiabatic quantum optimization with qudits," Quantum Information Processing 12(4), 1819–1829 (2013).

[14] IBMQExperience, <https://quantumexperience.ng.bluemix.net/qx/devices> (15 July 2018).

[15] Xu, N., Zhu, J., Lu, D., Zhou, X., Peng, X., and Jiangfeng Du, "Quantum Factorization of 143 on a Dipolar-Coupling Nuclear Magnetic Resonance System," Phys. Rev. Lett. 109, 269902 (2012).

[16] Dattani, N. S. and Bryans, N., "Quantum factorization of 56153 with only 4 qubits," 27 Nov. 2014 <https://arxiv.org/pdf/1411.6758.pdf> (15 July 2018).

[17] Shor, P. W., "Algorithms for quantum computation: discrete logarithms and factoring," Proceedings of the 35th IEEE Annual Symposium on Foundations of Computer Science (SFCS '94), 124–134 (1994).

[18] Cerf, N.J., Bourennane, M., Karlsson, A. and Gisin, N., "Security of quantum key distribution using d-level systems," Physical Review Letters 88(12), 127902 (2002).

[19] Shor, P.W. and Preskill, J., "Simple proof of security of the BB84 quantum key distribution protocol," Physical review letters, 85(2), 441 (2000).

[20] Zhao, Y., Fung, C.H.F., Qi, B., Chen, C. and Lo, H.K., "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems," Physical Review A 78(4), 042333 (2008).

[21] Hubbard, W. B., "Ice Giants Decadal Study," Planetary Science Decadal Survey, Mission Concept Study Final Report, NASA, (2010).

[22] Pecora, L. M. and Carroll, T. L., “Synchronization in Chaotic Systems,” Physical Review Letters 64(8) 821-824 (1990).

[23] Carroll, T. L. and Pecora, L. M., “Synchronizing chaotic circuits,” IEEE Transactions on Circuits and Systems 38, 453-456 (1991).

[24] Pecora, L. M. and Carroll, T. L., “Driving Systems with Chaotic Signals,” Physical Review A: Atomic, Molecular and Optical Physics 44, 2374-2383 (1991).

[25] Cuomo, K.M. and Oppenheim, A.V., “Circuit Implementation of Synchronized Chaos with Applications to Communications,” Physical Review Letters 71(1), 65-68 (1993).

[26] Cuomo, K.M., “Analysis and Synthesis of Self-Synchronizing Chaotic Systems,” Ph.D Dissertation, Dept. Elect. Eng. & Comp. Science, Massachusetts Institute of Technology, Cambridge, 1994, <http://www.rle.mit.edu/dspg/documents/KCuomoThesis.pdf > (15 July 2018).

[27] Bennett, C.H. and Brassard, G., “Quantum cryptography: Public key distribution and coin tossing,” Theor. Comput. Sci. 560(P1), 7-11 (2014).

[28] Yang, T., “A survey of chaotic secure communication systems,” International Journal of Computational Cognition 2(2), 81-130 (2004).

[29] Argyris, A., Syvridis, D., Larger, L., Annovazzi-Lodi, V., Colet, P., Fischer, I., Garcia-Ojalvo, J., Mirasso, C. R., Pesquera, L. and Shore, K. A., “Chaos-based communications at high bit rates using commercial fibre-optic links,” Nature 438(17), 343-346 (2005).

[30] Illing, L., “Digital Communication using Chaos and Nonlinear Dynamics,” Nonlinear Analysis: Theory, Methods & Applications 71(12) e2958–e2964 (2009).

[31] Zaher, A. A., Abu-Rezq, A., “On the design of chaos-based secure communication systems,” Communications in Nonlinear Science and Numerical Simulation 16(9), 3721-3737 (2011).

[32] Kapitaniak, T., Maistrenko, Y. and Grebogi, C., “Bubbling and riddling of higher-dimensional attractors,” Chaos, Solitons & Fractals 17(1)61-66 (2003).

[33] Annovazzi-Lodi, V., Aromataris, G., Benedetti, M. and Merlo, S., “Secure Chaotic Transmission on a Free-Space Optics Data Link,” IEEE Journal of Quantum Electronics 44(11), 1089-1095 (2008).

[34] Lang, R. and Kobayashi, K., “External optical feedback effects on semiconductor injection laser properties,” IEEE J. Quantum Electron 16(3), 347–355 (1980).

[35] Marcikic, I., Lamas-Linares, A. and Kurtsiefer, C., “Free-space quantum key distribution with entangled photons,” Applied Physics Letters 89(10), 101122 (2006).

[36] Schmitt-Manderbach, T., Weier, H., Fürst, M., Ursin, R., Tiefenbacher, F., Scheidl, T., Perdigues, J., Sodnik, Z., Kurtsiefer, C., Rarity, J.G. and Zeilinger, A., “Experimental demonstration of free-space decoy-state quantum key distribution over 144 km,” Physical Review Letters 98(1), 010504 (2007).

[37] Hughes, R.J., Nordholt, J.E., Derkacs, D. and Peterson, C.G., “Practical free-space quantum key distribution over 10 km in daylight and at night,” New journal of physics 4(1), 43 (2002).

[38] Cornwell, D., Boroson, D., Robinson, B., Burianek, D., Murphy, D. and Khatri, F., “The Lunar LaserCommunication Demonstration (LLCD),” NASA, 11 June 2014, <https://alumni.jhu.edu/sites/default/files/inline-images/NASA-LasercomTalk-JHU-Aerospace-Affinity-June-11th-2014.pdf> (15 July 2018).

[39] “GRACE (Gravity Recovery And Climate Experiment),” Earth Observation Portal, <https://directory.eoportal.org/web/eoportal/satellite-missions/g/grace> (15 july 2018).

[40] Hong-Wei,L., Zhen_Qiang,Y., Shuang,W., Yong-Jun,Q., Guang-Can, G., Ahen-Fu, H., “Randomness determines practical security of BB84 quantum distribution”, Nature Scientific Reports (5),16200(2015)

[41] NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations.