doi: 10.17586/2226-1494-2022-22-1-101-113

An optimal swift key generation and distribution for QKD

Mallavalli Raghavendra Suma[1]✉, Perumal Madhumathy[2]

[1] Dayananda Sagar College of Engineering, Bengaluru, 560078, India
[2] RV Institute of Technology and Management, Bengaluru, 560076, India

[1] sumamrvp@gmail.com✉, https://orcid.org/0000-0002-2842-0942
[2] Madhumathyp.rvitm@rvei.edu.in, https://orcid.org/0000-0003-2803-3712

Abstract
Secured transmission between users is essential for communication system models. Recently, cryptographic schemes were introduced for secured transmission and secret transmission between cloud users. In a cloud environment, there are many security issues that occur among the cloud users such as, account hacking, data breaches, broken authentication, compromised credentials, and so on. Quantum mechanics has been implemented in cryptography that made it efficient for strong security concerns over outsourced data in a cloud environment. Therefore, the present research focuses on providing excellent security for cloud users utilizing a swift key generation model for QKD cryptography. The Quantum Key Distribution (QKD) is an entirely secure scheme known as Cloud QKDP. Initially, a random bit sequence is generated to synchronize the channel. An eavesdropper will not permit to synchronize parameters between them. In this key reconciliation technique, the random bit sequence is concatenated with the photon polarisation state. BB84 protocol is improved by optimizing its bit size using FireFly Optimization (FFO) at the compatibility state, and in the next state, both transmitter and receiver generate a raw key. Once the key is generated, it is then used for the transmission of messages between cloud users. Furthermore, a Python environment is utilized to execute the proposed architecture, and the accuracy rate of the proposed model attained 98 %, and the error rate is 2 %. This proves the performance of the proposed firefly optimization algorithm based swift key generation model for QKD performs better than previous algorithms.

Keywords
cryptography, quantum mechanics, quantum key distribution (QKD), eavesdropper: BB84 protocol, reconciliation and firefly optimization

For citation: Suma M.R., Madhumathy P. An optimal swift key generation and distribution for QKD. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2022, vol. 22, no. 1, pp. 101–113. doi: 10.17586/2226-1494-2022-22-1-101-113

УДК 004.056

Оптимальная быстрая генерация и распределение квантовых ключей

Маллавалли Рагхавендра Сума[1]✉, Перумал Мадхумати[2]

[1] Инженерный колледж Даянанда Сагар, Бангалор, 560078, Индия
[2] RV Институт технологий и менеджмента, Бангалор, 560076, Индия

[1] sumamrvp@gmail.com✉, https://orcid.org/0000-0002-2842-0942
[2] Madhumathyp.rvitm@rvei.edu.in, https://orcid.org/0000-0003-2803-3712

Аннотация
Защищенная передача данных между пользователями важна для систем связи. Большое распространение получили криптографические схемы для защищенной и скрытой передач информации в облачной среде между пользователями. В данной среде возникает множество проблем с безопасностью, такие как взлом учетных записей, утечка данных, нарушение аутентификации, скомпрометированные учетные данные и др. Применение принципов квантовой механики в криптографии повысило ее эффективность для решения проблем безопасности данных, передаваемых на аутсорсинг в облачной среде. В работе предложено решение обеспечения повышенной безопасности для пользователей облачных сервисов за счет применения модели быстрой генерации ключей

для криптографии Quantum Key Distribution (QKD). Квантовое распределение ключей представляет собой безопасную схему, известную как Cloud QKDP. Для синхронизации канала генерируется случайная битовая последовательность при этом злоумышленник не может синхронизировать параметры между каналами. В методе согласования ключей случайная битовая последовательность объединена с состоянием поляризации фотона. Первый протокол квантового распределения ключей BB84 улучшен за счет оптимизации его битового размера с помощью FireFly Optimization в состоянии совместимости. В следующем состоянии передатчик и приемник генерируют необработанный ключ. Далее с помощью ключа выполняется передача сообщений между пользователями облака. Для реализации предложенной архитектуры использована среда Python. Точность представленной модели достигает 98 %, а уровень ошибок не превышает 2 %. Выполненные эксперименты показали, что модель генерации ключей Swift на основе алгоритма оптимизации Firefly для QKD работает эффективнее, чем известные алгоритмы.

Ключевые слова
криптография, квантовая механика, квантовое распределение ключей (QKD), перехватчик: протокол BB84, согласование и оптимизация Firefly

Ссылка для цитирования: Сума М.Р., Мадхумати П. Оптимальная быстрая генерация и распределение квантовых ключей // Научно-технический вестник информационных технологий, механики и оптики. 2022. Т. 22, № 1. С. 101–113 (на англ. яз.). doi: 10.17586/2226-1494-2022-22-1-101-113

Introduction

Communication, the ability to interact in a secure manner, is an essential feature of humanity. Traditional communications fall on the computational complexity of mathematical models. A major problem that is involved here is the factorization of Prime numbers, and researchers work on it to develop a solution for this issue in less exponential time [1]. Quantum computers are used for solving this issue in polynomial time and made it feasible that encryption depends on hardware difficulty of mathematical tasks [2]. This resulted in turning the focus over physical laws to encode the messages, and a foundation type of key distribution algorithm has been developed previously. By establishing a key between a transmitter and receiver, the communication was made efficient and secure. Security of the protocol is realized only when linear and diagonal methods are implemented and analyzed for transmitting information [3]. In order to ensure security, different algorithms such as Elliptic Curve Cryptography (ECC) [4], Hash function cryptography [5], symmetric or asymmetric type cryptography [6] schemes use selective access control and digital signatures. These schemes were found to have some drawbacks such as being difficult to access by the user, and more methods are added to protect vulnerability. These controls are left only to admins for increasing the computational cost by solving mathematical issues, which can also increase computational power [7].

The requirement of a communication model is based on the idea that a user allows parties to establish keys and track the security of the communication channel. Tracking was done by estimating error and noise values caused during communication [8]. Active hackers were capable to catch transmitted messages, and therefore the only way was to secure the message during transmission. Security of cryptography has been measured as strong or weak with respect to time and resources that is required to recover a plain text. Analyzing a ciphertext obtained by a strong cryptography technique, it might be very difficult to decipher it without an appropriate decoding tool [9] that requires computing power and time, with many computers doing analysis in a second. It is impossible to decipher the result of finite cryptography that will not allow intruders to determine messages [10].

Many researchers have been focused on building the strongest encryption methods with respect to computing power. In a cryptographic algorithm, a cypher is a mathematical function used for the encryption and decryption process. It works with a combination of the key, and the key may be in the format of word, number or phrase for encrypting the plaintext [11]. Plaintext encrypt different ciphertext in different techniques using keys. Security of encrypted data is based on the strength or length of the algorithm and the secrecy of the key. Conventional algorithms such as Rivest-Shamir-Adleman (RSA), ECC and Financial Service Authority (FSA) algorithms use the key for encrypting data by an agreement protocol. The key is shared between the transmitter and receiver, and then the message is conventionally encrypted in the communication channel [12]. The sender and the receiver must keep the secret key within themselves. To prevent the secret key from getting disclosed during transmission, different neural network schemes have been implemented previously. An intruder might be able to intercept with the key and read, modify and collapse the data format at the receiver. An authenticated key gets the most attention in the conventional methods. In order to overcome the drawbacks caused by using key encryption stages, a request on security-based transmission protocol have been raised [13]. As the key size and message size length took over all the memory. However, there remains a public key for user access which is mathematically related to deriving message bits when given enough time and computation power.

Cryptography is the method of acquiring confidential data with the help of mathematical equations. Intruders might find different ways to conquer secrets, and instead, researchers developed powerful techniques to compromise the intruders via secured communication. Security threat pushed over Quantum mechanics on Cryptography. Quantum computation is posed on cryptographic schemes that are based on assumptions like factorization problem and discrete logarithm problem. RSA technique is used for purposes in e-commerce [14]. Some basic physics used in cryptographic security made Quantum Cryptography a promising scheme. In quantum key distribution, and ideally in other quantity encryption applications, any assaults permitted under quantum mechanics are assumed to have a security result. Quantum Key Distribution (QKD) secures information by sharing secured key to the sender and receiver. It becomes crucial to prevent guessing of the key from an eavesdropper. Proper encryption and decryption are essential to prevent Eve from guessing the key since it requires a lot of effort to overcome the drawbacks of QKD to make it practically applicable. A change in photon might affect the message passing through certain materials, and digital signature authenticates the communication channel at the receiver side.

The digital signature process is composed of three key generations, key verification and signature algorithms. These algorithms are essential for real-time tools to be implemented. QKD requires many features for certifying a channel for communication before transmission. Recent research has shown that QKD is efficient at a speed of 16 bits per second at a distance of 256 km, which demands many repeaters and increases the communication costs. Thus, an accurate communication channel for long-distance that minimized repeaters is required. Exchanging data using a single photon requires a dedicated, high-quality channel, and so the transmission of keys from the Quantum channel to two or more sites is impossible because they contradict Quantum principles. The number of tests required to transmit a photon without absorption and depolarisation increases and consumes much time exponentially with regard to the channel length. Error probabilities require a measurement scheme unless this execution takes a long time and power. The physical application of the protocol is a major step towards verifying a communication system. This will include the analysis of state preparation uncertainties, which will result in additional errors. Thus, these drawbacks in the QKD scheme motivated to design an optimal solution to measure the error between a sender and receiver, thus enhancing the channel efficiency for secured communication.

The main contributes of the proposed model are given below.

- To attain secure data transmission in cloud computing, an effective optimal swift key generation technique is introduced.
- To achieve improved key generation and distribution techniques for cloud users, a QKD protocol with its quantum mechanism is developed.
- To attain a fast key generation, the model utilizes Firefly Optimization Algorithm (FOA) optimization.
- For selecting the appropriate block size, an optimization scheme of Frequency Fitness Assignment (FFA) is implemented in this model to make it useful for obtaining the best key pair.
- To verify and evaluate the proposed model, the simulation is accompanied to prove the proposed model.

Literature review

Different Cryptographical schemes are presented in various works in order to provide secure communication. Below, we discuss some of them and their drawbacks.

Chan et al. [15] have presented Identity Based Cryptography that have public key certification. It was used in a Mobile Adhoc Network (MANET). This method has been designed particularly for bi directional channels as they rarely exist in MANET. However, this algorithm requires a centralized server for private key issues for various identities and gives a protocol for sharing this task between users. This remains a drawback for using it in MANETs. Jin et al. [16] have investigated pairwise key generation in dynamic wireless networks with a central node and random user arrival. The establishment of a key generation model for this type of network was done depending on the discrete Markov chain to compute the average time per user spent on completing and waiting for key generation. It was able to tackle both parallel and serial key generation scheduling under different conditions. However, it exploited various wireless broadcast characteristics to reduce probing energy was a drawback.

Wang et al. [17] have described multivariate public key cryptosystems that depend on Clipped Hopfield Neural Network and use them in video framework executed at search space. In the matrix field, Diffie-Hellman key exchange algorithm is lengthened into a matrix field that illustrated feasibility unwanted for specific applications for post-quantum cryptography and classic cryptography. However, it required multivariate public key cryptosystems that permit hardware realization in real-time applications. Xu et al. [18] have investigated secret key generation issues for various types of wireless networks by exploring them in physical layer features of wireless channels. Key generation parameters with low complexity have been proposed that combined point-to-point pairwise key generation method, multi-segment method and onetime pad. Specifically, group key generation methods were studied for three types of networks such as three-node, multimode and multimode mesh. However, it has been reduced by the maximum time allocation issue and reformulated into series programming.

Howe et al. [19] have presented discrete Gaussian Samplers for lattice-based cryptography that targeted physical devices. Discrete Gaussian sampler hardware has been used as the main sampling method, and it aims to offer security against side-channel timing attacks using discrete Ziggurat sampler hardware designs. However, due to non-constant time characteristics of rejection, sampling buffers are implemented between each element that permits parallel execution that acquires maximum computation cost of every component.

Dey et al. [20] have presented a lightweight and secure session key establishment scheme for smart home networks and used Diffie Hellman key exchange as an alternative technique. It established a public key between the home gateway and smart device. However, it completely integrated society into its security concerns, and its measurements were noted rather found that it exhibits very contrasting security protocol that was hard to be implemented in real-time applications.

Zhang et al. [21] have symmetrically investigated the secret key capacity of key generation from wireless channels by considering sampling delay impacts from intruder's source model and found that secret key capacity is predicted by cross-correlation coefficients of channel measurements as it does not require a legitimate channel. By analyzing Doppler spread, pilot length and key generation parameters, it attempts to achieve secret key security. However, if the message data get leaked to eavesdroppers, it might decrease key capacity and also fails to provide a legitimate communication channel to users.

He et al. [22] have presented an in-depth security protocol of ECC based Radio-Frequency Identification (RFID) schemes that predicted some of the security requirements that satisfied authentication schemes. It analyzed the communication cost and security requirements of this protocol and found that it required authentication schemes that satisfy security requirements. However, this method of ECC-based RFID scheme has unacceptable communication cost and computation complexity that was left unused in IoT applications. Furqan et al. [23] have presented a secret key generation algorithm for wireless channels in multicarrier systems for ensuring confidentiality in wireless communication systems. Secret bits are generated randomly from both magnitudes of orthogonal frequency division multiplexing sub channels also from its position with respect to maximum gains. Mismatch rate and key generation rate have been evaluated in this algorithm. However, unfortunately, it extended dimensions for a secret key generation that, in turn, increased the cost of the algorithm.

Almajed et al. [24] have introduced Se-Enc Scheme that was based on ECC that encodes messages effectively to map them in an elliptic curve. It skipped the encoding phase that resisted encryption attacks, and its security analysis illuminated the degree to which it remained secure. It analyzed padding sizes, number of encoding operations and attacks with respect to decoding operations. However, the performance evaluation of this scheme has failed to provide efficient security over transmission.

Problem statement

Quantum computers are extremely complex to design, manufacture and operate. Consequently, they are hobbled by flaws such as noise, malfunctions, and the loss of quantum coherence, which is critical to their operation but breaks down before any non-trivial process is complete. Due to the various random channels linked with these terminals, the key generation among a group of terminals is more complicated. Hence, numerous tree-based techniques have been devised to achieve the multi-terminal pairwise independent network's group secret key capacity. Quantum cryptography can be used to solve this problem. The Quantum Key Distribution Protocol for Secure Cloud Computing, which uses quantum principles to secure cloud storage and data dynamics, was previously introduced with certain disadvantages, including formal key creation that takes years and an agreement foundation. Cloud computing security does not have to be confined by quantum cryptography. During data transfer, there is a high risk of data being intercepted by an eavesdropper. Therefore, research focuses on the development of an improved cryptography technique for secure and secret transmission in a cloud environment.

Furthermore, this research demonstrates the application of quantum computing features, which is a domain that uses photonics to communicate via protocols. This computer technology provides a security feature that is free of all risks and far more powerful than the protection approaches utilized in ubiquitous computing previously. Because data encryption in any device wraps confidential and personal data with a higher level of protection and security, data should be safe from attacks. Cryptographic methods such as ECC, Chaotic secured Cryptography and RSA algorithm used a key to make transmission secure. However, these algorithms have the necessity of sharing a key between a sender and receiver to make the transmission. This remains a way for intruders to attack. The Quantum Key Distribution Method is a cryptography system that leverages unusual features to share sensitive and confidential data. This key is used to encrypt data that will be communicated between concerned parties in an insecure manner.

Proposed FOA-QKD model

FOA based QKD (FOA-QKD) is a secured communication model that uses proper channel synchronization is a major objective of this work. By implementing QKD protocol with its quantum mechanics, it has been acquired to gain its benefits for efficient communication. Message bits are encrypted using encryption operators and converted to *qbits* as per BB84 protocol. This protocol works as per cryptography rules and also performs analysis over the transmission in order to check whether it is appropriate to transfer data with the obtained key. The key is obtained by estimating errors and optimizing them below the threshold. The length of key bits is minimized twice in order to use it as a key for encryption during further transmission. All other values are eliminated from the sender and receiver sides for security purposes.

Quantum cryptographic constructions for FOA-QKD

QKD is constructed using a random photon generator that emits photons in free space where they acquire different polarisation states. The polarisation states are measured using emitter state analysis. In this proposed model, a one-photon source model with radiative cascade has been used, and this is generated using a single-photon source emitter. The ability to produce single photons are described at relevant degrees. Using probabilistic photon sources, photon pairs with spontaneous non-linear optical processes are evaluated. QKD first develops a set of binary values such as 1's and 0's randomly, and every value from these binary digits is chosen from the transmitter for sending data from two polarisation bases. The polarisation bases can be given as $\{|0>, |+>\} = 1$; $\{|1>, |->\} = 0$. The basic structure of the proposed quantum cryptography is show in Fig. 1.

Photons are randomly measured, and their polarisation state is monitored from one of the Deux bases. By defining a key, the receiver uses a traditional communication system to recognize transmitters. Then it analyzes each photon of the transmitter's, which has been measured in polarisation basis, as well as analyzes the base agreement determined

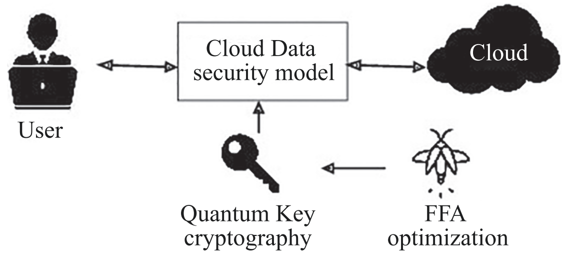

Fig. 1. Quantum Cryptography basic structure

by the protocol in its initial state. The quantitative portion of the QKD protocol is called Alice and Bob encoding and decoding. By assuming that Alice uses *m* different encodings with index from BB84 protocol and each state is denoted as encoded bit values of 0 and 1. In the first step of the protocol, Alice randomly selected *n* bits and *n qbits* prepared in the states to Bob for randomly chosen encoding technique. Each photon contains a quantized amount of energy determined by the photon wavelength. The total energy of 2.5 J is obtained by the addition of many photons.

$$E = hf = h\frac{c}{\eta}. \tag{1}$$

In equation (1), E represents the energy of a single-photon, and its wavelength is denoted as η. c is the number of photons and h gives Planck's constant, f is frequency range. By receiving these states that were perturbed received or attacked, Bob applies its measurements to gather classical bits. At last, Alice and Bob employ measurement operations that are compatible. Photons were then measured with the correct benchmark, and the raw key for encryption was generated. This benchmark allows the measurement and communication to establish key and track the security of communication channels.

BB84 protocol

Encode each secret key bit into the single-photon polarisation state. Due to the polarisation states of a single photon, this data was left "fragile" and will be unavailable for eavesdroppers unless this photon was destroyed. Every eavesdropper detects photons and then sends them back to the receiver. But, resendding of this photon, the eve will send them with a wrong polarisation state. This helps to reveal that the eve is present at this communication. Thus, while Alice sends a sequence of pulses that contain single-photon polarised differently, Alice encodes them as Zeroes into *H*-polarised photons and unit as *V*, other half bits are selected randomly and encoded in diagonal polarisation basis, as *D* represents zero and *A* as unity.

State of photon polarisation enhanced in FOA-QKD.

Alice produces an unknown quantic state sequence $\{|x, + | > (k = 1, 2, \ldots, m)\}$. Next, Alice performs a unique transformation in this sequence in all quantum conditions. It is defined as shown in the below equation:

$$\begin{bmatrix} D & H \\ V & A \end{bmatrix}.$$

Apparently, Alice gets a qubit state sequence for unitary information of 1 qubit, then Alice might share the unknown states sequence by following steps.

1. Alice selects and inserts certain particles into the sequence to represent the states of polarisation. Initial state records have been made regarding each decoy particle's position. Alice sends the sequence to Bob, then reports the position of the respective bases and publishes its results.
2. In comparison with the initial states, Alice calculates the probability of an error, and the value of an error is lower than the threshold value. Alice declares that the process is efficient, and this process continues or that the sequencing process is discarded and a new one begins. This process is called an analysis of security.
3. After sequence extraction from the received sequence was performed, the deletion of decoy particles took place, and the sequence took place in a quantum state.
4. Bob randomly picks and inserts some decoy particles in the sequence from the state.

Every decoy particle transmits sequence with respect to its state by recording its initial state and its respective places. Similar to Alice, Bob performs security checking. Comparison between these security analyses results is shown below in Table 1.

This polarisation state, as shown in Table 1, is measured at the receiver side and constructed with its respective volume. Horizontal (*H*), vertical (*V*), diagonal (+45°) (*D*) and anti-diagonal (–45°) (*A*) are the four equal random polarisation states that Alice can select for each bit. On the receiver side, Bob measures polarisation using a standard set up and this way, Bob distinguishes between *H* and *V* polarisation that is used on an *HV* basis. In half of the cases, Bob randomly changes his basis to other random formations. After transmitting a certain number of bits, Bob announces the basis he used for each bit. Then Alice says the cases that are on the same basis. Different bits are then thrown out for optimal key generation.

Key generation

Distributing the photon pairs ensures the highest possible compatibility to the polarisation state. In this case, synchronization between Alice and Bob, knowledge about photons arrival time at nodes and distance between Alice and Bob is essentially known. The strong polarisation correlation between emitted photons and the influence of noise in photons is clearly understandable for key generation. In order to make key generation efficient, Polarisation Dependent Loss (PDL) and Polarisation Mode

Table 1. Polarisation state and qubit assignation

Alice's random bit	0	1	1	0	1	0	0	1	0	1
Alice's random sending basis	×	+	×	+	+	×	+	×	+	+
Photon Polarisation Alice sends	*D*	*H*	*A*	*H*	*V*	*D*	*H*	*A*	*H*	*V*
Qubit generation	↑	→	←	→	↓	↑	→	←	→	↓

Dispersion are assumed to be null. PDL, due to its coherent properties, does not affect key generation as QKD chooses a time bin equal to 1ns and is used for determining the decoy period. This process appears to filter out the majority of background photons and ambient light, but it still considers 97 per cent of photons and does not filter the signal.

Fig. 2 displays the raw key rate, which averaged 135 bits per second during a 13-hour period. The extraction and collecting efficiency of the photons, as well as other concessions made within the experimental setup, limit the bit rate in our experiment. Blinking is another factor, as it reduces the per cent of the time that the quantum dot (QD) is optically active to roughly 0.3 for the QD employed here. Initially, in the key generation phase, the sequence of the polarisation state is shared over the quantum channel, and it results in an array of polarisation states on the receiver side. This state is then used for raw key generation. Raw key generation occurs at both Alice side and Bob's side, error values that occur during this synchronization time are then predicted at the error presumption phase and eliminated assuming that other bits are subjected to the risk state of an eavesdropper.

Error presumption

Quantum mechanics provides actual randomness derived from physical rules. Sending a photon through a 50:50 beam splitter and placing two single-photon detectors on the two outgoing arms is a straightforward technique to make a quantum random number generator. The generated (0 or 1) bit value is determined by which the detector detects a photon. Post-production procedures are used to repair faults in the quantum transmission and erase any leftover information that the eve could have on the raw key, processes including post-selection of data, error correction, and privacy amplification. The end result is a key that Alice and Bob share, but which Eve very probably has no knowledge of. The computational complexity of traditional post-processing techniques, as well as the necessity to process large amounts of raw data in a short amount of time, are currently hurdles in high-speed QKD. As seen in pseudocode 1, a comparison of Alice's raw key and Bob's raw key was performed.

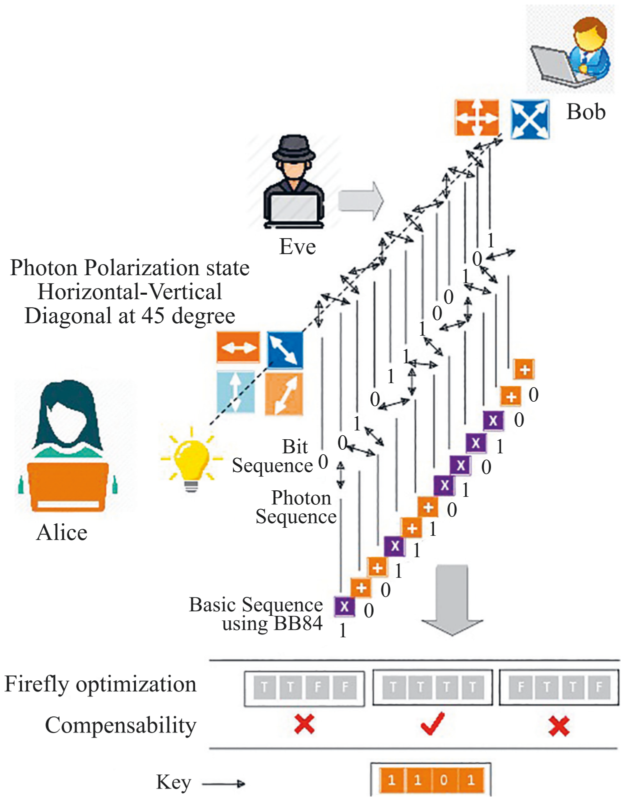

Fig. 2. Key generation architecture

Pseudocode 1. Error Presumption

```
Alice's key = hex1.(into binary)
Bob's Key = hex2.(into binary)
long int i = 0; j= key length;
get (hex1,hex2)
get("%s",hex1);
Out ("\n Equivalent binary value: ");
while (hex1[i])
if
hex1[i]= hex2[i]
Out > True
else
Out> False
```

Error elimination using optimization

Alice and Bob have a secret channel through which Alice sends Bob an *n-bit* string. Following that, Bob receives an *n-bit* string *B* that an eavesdropper with unlimited computing power may obtain by listening to the public channel. Alice and Bob's algorithms define the reconciliation protocol. It runs between strings to establish a public channel for sharing information. The amount of leaked information is the amount of data that an Eavesdropper could gather on *S* with *Q*. To accomplish key reconciliation, Alice and Bob pick a random function from a list of *n* functions with an unknown *m* parameter. This function is shared with the public. On the public channel, Alice transmits this function to Bob. When Bob decodes this string, he gets a string with the shortest distance between all strings. Alice and Bob decide on *k*1 and partition their string into *k*1 bit blocks. In pass 1, the bits in each position are in the form of block *v*. Alice sends Bob parties made out of all of her blocks. Each block whose parity differs from Alice's block is corrected by using Binary Bob. All of Bob's blocks have the even number of mistakes at this point, particularly zero. In this publication, leaked information about the secret string is removed during execution by eliminating one bit from each subset for which parity is known. This information can be saved for each transfer and used to fix errors. Specific block size is chosen so that the probability of a block having one or more errors decreases exponentially as the number of pathways increases. On blocks generated by concatenating a large number of blocks, large enough blocks are employed to completely eliminate errors.

1. Objective function

   The objective function is to find the best block size for portioning the message bits for comparison in order to obtain the best key pair. To find a solution that includes both the error value and the optimal key combination, the Firefly algorithm (FA) is employed to optimize this multi-objective function. The objective function is given as below:

$$F = F_{\min}[F_1]. \qquad (2)$$

From equation (2), F_1 represents sub-objective functions and the main objective function is represented by F.

2. Reduction of F_1

The first sub-objective function is represented in the following equation:

$$P(e) = C_k\, \mathcal{E}(1 - \mathcal{E})^{k-e}. \qquad (3)$$

In equation (3), $\mathcal{E}$ denotes error rate, C_k is the current error rate and e is the exact errors. Possibility for an odd number of errors can be given as:

$$P_{odd} = \sum_{i=1}^{\alpha} P(2i - 1) = \frac{1 - (1 - 2\mathcal{E})^k}{2}. \qquad (4)$$

There are proportions for the total number of errors in equation (4) and the expectation of the number of errors can be given as

$$\frac{N}{K} P_{odd} = \mathrm{E}\ .$$

The number of errors expected here is as follows:

$$F_1 = \frac{\mathrm{E}}{N\varepsilon} = \frac{1 - (1 - 2\mathcal{E})^k}{2\varepsilon k}. \qquad (5)$$

In equation (5), ε is the error rate, K is the block size, N is the key length and errors are assumed to be below the threshold value. The following is explained by the detailed application of the proposed Firefly algorithm.

3. Firefly algorithm

The FA is a search algorithm that uses flashing lights released by a biological process to identify fireflies insects. The intensity of the shining light can be thought of as one of the key enticing communication signals used to attract other fireflies. The process flow of the firefly optimization algorithm is illustrated in Fig. 3. The characteristics of fireflies are summarized here.

- Regardless of their nature, all extant fireflies aim to attract other fireflies.
- The attractiveness of a firefly is proportional to the amount of light it emits and the intensity of that light.
- When two glowing fireflies are present, the one with the less lighting firefly travels toward the one with the better glowing firefly.
- If their intensities are the same, they will move around in a different search space at random.
- The objective function determines the intensity of the firefly light.

The FA technique has two main issues: light intensity discrepancy (I) and attractiveness quantity (β). The light intensity $I(r)$ fluctuates non-linearly (exponentially) with the distance r as follows:

$$I(r) = I_0 e^{-\gamma r}, \qquad (6)$$

In equation (6), I_0 → initial light intensity; γ → light absorption coefficient; β → attractiveness.

The β is given as:

$$\beta = \beta_0 e^{-\gamma r},$$

where attractiveness is given as β_0 at $r = 0$. The displacement of any two fireflies S_i and S_j is given by an empirical formula known as Euclidean distance as follows:

$$r_{ij} = \|S_i - S_j\| = \sqrt{\sum_{k=1}^{k=n} (S_{ik} - S_{jk})^2}.$$

The dimension of the problem is defined by the number 'n'. As a result, an expression is used to characterize the total movement:

$$S_i = S_i + \beta_0 e^{-\gamma r_{ij}^2}(S_i - S_j) + \alpha\varepsilon_i. \qquad (7)$$

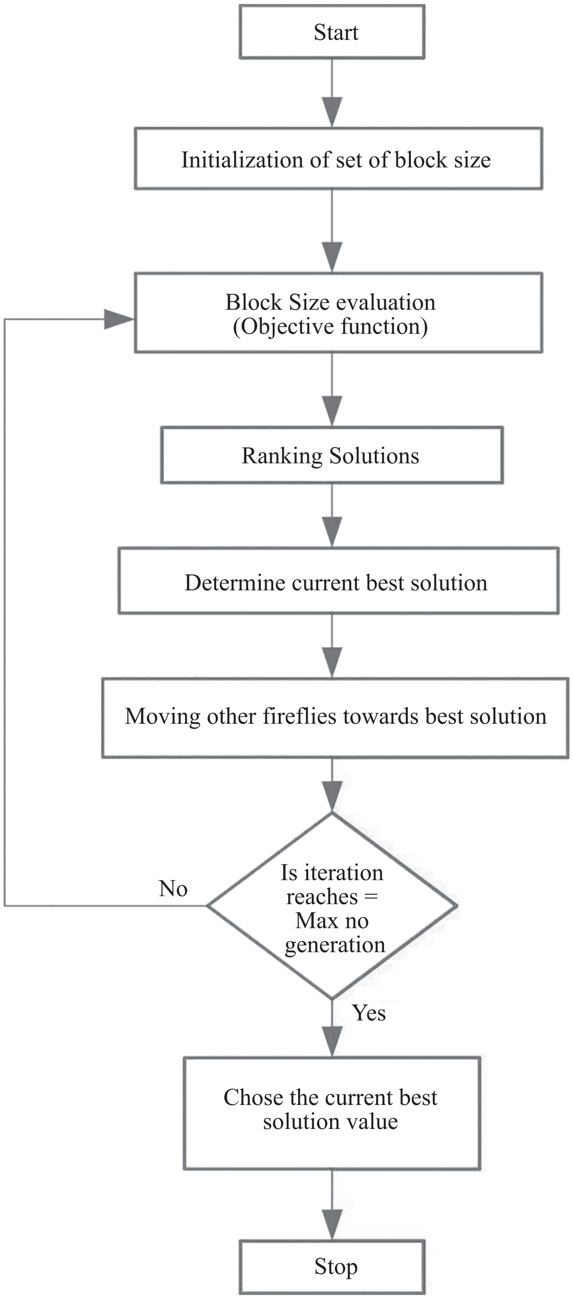
Start
Initialization of set of block size
Block Size evaluation
(Objective function)
Ranking Solutions
Determine current best solution
Moving other fireflies towards best solution
Is iteration reaches = Max no generation
No
Yes
Chose the current best solution value
Stop

Fig. 3. Flow-chart of the firefly optimization algorithm

From equation (7), γ represents the most important parameter in the firefly algorithm, ε_i is a vector of random numbers being drawn from a Gaussian distribution or uniform distribution and a random walk partial towards the brighter fireflies like if $\beta_0 = 0$. Another more beautiful firefly *j* directs the movement of the i^{th} firefly. Firefly movements can have one of three forms:

The current position in the firefly i^{th}.

Migrating to a more appealing firefly.

Random motion depending on the number and α and εi randomly created by the parameter [0; 1].

Privacy amplification

At this point, Alice and Bob both have the same strings, but they are not private in the entire. There is a chance for the eve to gain some message about them by beam splitting or in the way of intercepting the data. Later one causes an error in Bob's string, and the eve might be able to use a small number of bits and induced errors get eliminated in error caused by physical devices and noise detectors present. Hence, during reconciliation the eve was not be able to get any information. Alice and Bob can use the beam intensity *m* and the bit error rate to calculate the expected fraction of F_1 that Eve has learned. If they are conservative in their assumptions and add several standard deviations to their results, they will have a safe upper bound on the number of bits leaked to Eve. Assuming that Eve knows only deterministic bits, so another issue is whether it might be more useful to her to obtain probabilistic information about *M* instead. Instead of measuring photons keeping the same base as Alice and Bob, a halfway can be picturized out by Eve. It might help her to find matches. Alice, with a maximum probability of about 85 %, is pointless in the case of Bob announcing that his measurement choices were left probabilistic rather than deterministic. The privacy amplification stage is measured using errors caused at Bob's side so as to predict the deterministic bits and thus to informally get the final key.

Proposed FOA-QKD protocol

The proposed model sends a message across a quantum channel, which is then utilized to run a system model to replicate and decode the message. In QKD cryptography, the transmitter is Alice, the receiver is Bob, and the eavesdropper is Eve, which are illustrated in Fig. 4.

- For synchronization, a set of possible parameters is chosen from the codebook, and Alice and Bob produce a set of subset parameters using a pre-shared secret.
- Following the development of a key agreement, Alice and Bob begin synchronizing the transmitter and reception stations in order to begin communication. During the execution of this process, essential system parameters such as channel propagation length are predicted. Synchronization between devices is left independent and used to compare photon states of them.
- With the use of the BB84 protocol, Alice begins key establishment and prepares a bitstream that is indicated as *Set A* with regard to the polarisation states of every photon.
- By establishing a time-bin system, Alice generated a random binary message, $M = \{m_0, m_1, \ldots, m_l\}$, *where* $m_{1\ldots l} = \{0 \textit{ or } 1\}$, encodes them using polarisation basis $\{A\}$ and its procedure is given in algorithm 1. The output of this encoding is the set $\{B\}$.
- Then Bob produced a set of measuring bases at random and labelled set *C* for each photon. During computation, the state of each photon is measured and recorded as $\{D\}$.
- This recorded state was then transmitted back to Alice. With the help of $\{A\}$ and $\{C\}$, Alice used certain protocols to estimate values between them, and Alice used these bits to establish the raw key $\{E_{Alice}\}$.
- Bob subsequently selects components of *D* indicated in Alice's communication and creates a raw key, then selects a tiny subgroup from *E* and communicates their states and locations back to Alice.
- Alice forecasts the key bits and relates them to Bob with the aid of this subgroup. Error estimation is performed at this stage by setting up of threshold value. If an error is below the threshold, the communication channel is then established; otherwise, an optimization is performed for the estimating error.

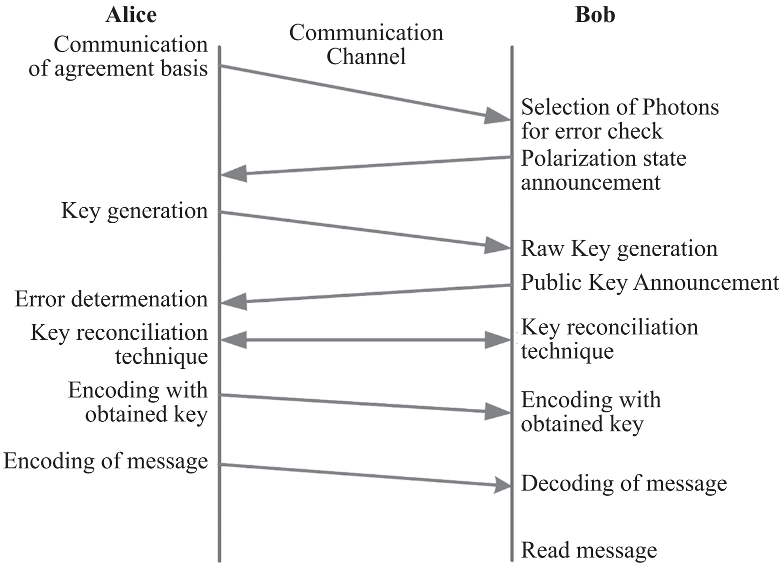
Alice
Communication of agreement basis
Communication Channel
Bob
Selection of Photons for error check
Polarization state announcement
Key generation
Raw Key generation
Public Key Announcement
Error determenation
Key reconciliation technique
Key reconciliation technique
Encoding with obtained key
Encoding with obtained key
Encoding of message
Decoding of message
Read message

Fig. 4. Communication protocol

- Additionally, a reconciliation technique to correct these errors was performed. A protocol, namely firefly optimization, is established to reduce this error between keys.
- Mayfly optimization presupposes that Alice's key, *EAlice*, and Bob's estimate of Alice's key, *EBob*, each have a source coding. Alice and Bob share *F*, where the comparison was made to check for error.
- Furthermore, the exchange of *F* between Alice and Bob causes inaccuracies that should be corrected. *FAlice* and *FBob* are the only ones left after the comparison. By continuously comparing subdivided blocks of communication, optimization reconciles mistakes between them. With a memory-less channel, a joint probability of *FAlice*, *Bob*=*y* occurs.

$$y = p(FAlice|FBob)p(FBob)$$

- Because *FAlice* and *FBob* are the same lengths, no additional coding bits are required in *F*, and the conditional data entropy between Alice and Bob on message *F* is *H*(*FAlice*|*FBob*), the reconciliation operation is efficient.
- Every iteration takes *F* and is subdivided into the blocks *K*, in which iteration is referred to by the subscript. Alice and Bob compute the copy of their i^{th} message on *n* blocks in every step. Blocks that vary via at least one error are divided continuously in the block between two users and calculated until all blocks are resolved. In the end, key *F* is used for cryptography by both users.
- Alice uses this encrypted solution after setting up a key. This key gain is applied by Bob to a binary string, converted back to a floating-point number to get the encrypted message.
- Following receipt of the encrypted message, Bob uses this key to obtain an appropriate binary string, converts it to a float number, and then obtains the answer.
- Privacy amplification can be achieved by appropriate random data compression or random universal hashing, which reduces the string to a sufficiently shorter one.

Results

Secured key generation and its performance are presented in this paper. Results were obtained by implementing the proposed scheme for selecting the optimal size of the block incompatibility state in order to obtain key values fast and thus improve the secrecy of the channel as far as possible. The proposed scheme is implemented in the Python environment of processor Intel ® Core TM i5-330S CPU @ 2.70GHz and 8GB RAM. Results are compared with previous methods such as C-QKD (Chaotic Quantum Key Distribution), CH-QKD (Chip-based QKD), Full Quantum one way QKD and Post Quantum Cryptography. The analysis involves measuring Accuracy, Error, Key generation rate, and eavesdropping rate. Table 2 illustrates the comparison between the proposed and existing algorithms.

Accuracy

Accuracy is measured with respect to the number of bits encoded and decoded appropriately. It can be described as a number of bits/messages transmitted with the fraction of a number of bits/messages received appropriately. Results are compared with previous methods and shown in Fig. 5.

From Fig. 5, one can see that the proposed model gets a higher accuracy rate of 98 % in the encoding and decoding stage analysis. By sending the number of bits at the encoding process and decoding those using the same technique, the accuracy level was reached at its maximum range. Compared with previous techniques, P-QKD reached 94 %, and C-QKD reached 89 % that was due to its key reconciliation properties. These methods use the traditional channel for transferring messages and thus fail to obtain a higher accuracy range. F-QKD reached 83 % of accuracy value, and CH-QKD reached 72 % of the accuracy range. Thus, the proposed technique has been efficient in terms of accuracy values.

Error

Error-values are measured as false identified bits at the decoder side with respect to encoder values. It can be given as a fraction between original values to the false identified values in the message. The values are measured and plotted in the graph, as shown in Fig. 6.

The graph suggests that the proposed FOA-QKD model exhibits less error value of 2 % due to its improvement in the key reconciliation scheme. P-QKD exhibits 6 %, and

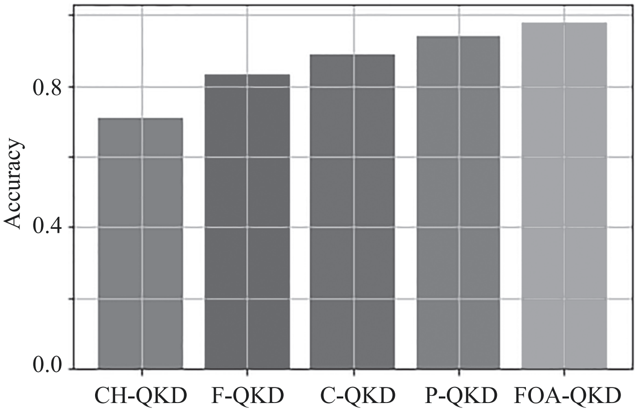

Fig. 5. Accuracy analysis of the proposed and previous methods

Table 2. Comparison between the proposed and existing algorithms

Performance metrics	CH-QKD	F-QKD	C-QKD	P-QKD	FOA-QKD
Accuracy	0.70	0.85	0.89	0.93	0.98
Error	0.28	0.17	0.11	0.06	0.02
Eve's dropping rate	0.81	0.78	0.75	0.68	0.65
Key Generation Time	170	168	167	163	162

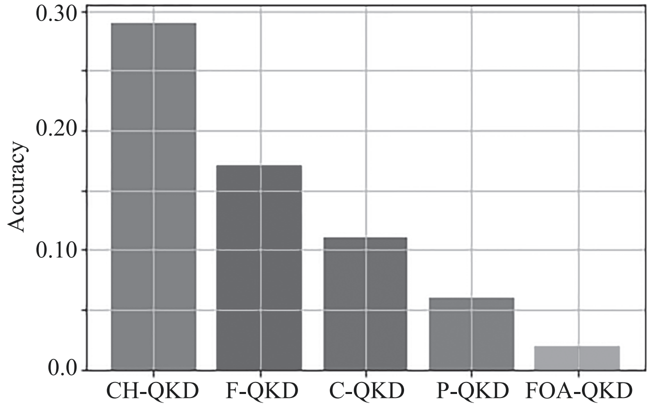

Fig. 6. Error analysis between the proposed and previous models

C-QKD gives 11 % of error. This was due to its traditional approaches over channel synchronization. F-QKD exhibits an error rate of 16 %, and CH-QKD gives an error value of 28 %. The proposed model was found to be error-resistant compared to other QKD techniques. Error-values are minimized due to properly secured transmission between encoding and decoding strategies of the proposed model. Similarly, a higher value of error in CH-QKD is due to its chaotic channel synchronization techniques that failed to minimize the error between information transferred.

Eve's dropping rate

Eve dropping rate was an important concern in the QKD protocol, as they are measured when errors are generated during raw key generation between Alice and Bob with respect to their shared information at the initial stage in order to synchronize channel and transmission rate. It is the ratio of the number of mismatching bits to the total number of extracted bits. To limit eavesdropper's knowledge of the key, both parties discard the last bit of their respective blocks. However, if the parity does not match, they discard the block entirely.

With respect to noise detectors and intruders attack like times attack and Brute-Force attack, eavesdropping rate was measured. From Fig. 7, the proposed model was found to be resistant to the attack and gives a minimum eavesdropping rate due to its enhanced method of announcing the polarisation state between Alice and Bob. FOA-QKD model generates an eavesdropping rate of 0.6 for 2 bits and similarly extends below 0.4 for 8-bits. It reaches 0.5 at a range of 125. Similarly, for previous methods such as P-QKD, C-QKD and CH-QKD, the values range between 0.8 to 0.65 rates and thus evaluated for 2-bit, 4-bit and continuously up to 125-bit.

Key generation time

The raw key was generated as per the proper synchronization of Alice and Bob during key reconciliation time. In the proposed FOA-QKD protocol, key generation time is measured from the time of sending random bit sequences to bob and correspondingly generating key values by eliminating errors between them.

Key generation rate is the measurement of the generation of keys and the fraction of time between them. It was measured for the proposed method as well as for existing methods. Fig. 8, *a* shows that the FOA-QKD model other exhibits very low key generation time for input message bytes of 2 to 125 bytes. Existing methods such as P-QKD exhibits a difference of 0.02 rate values with respect to FOA-QKD. C-QKD and F-QKD need a long key generation time due to their complex protocols for key generation. The rather proposed model used an enhanced format of BB84 protocol for exhibiting key values. CH-QKD protocol then founds its key generation time far greater than all other methods for key generation. In Fig. 8, *b*, the proposed model key generation time was shown. From the figure, it was examined that key generation was found to be linear throughout all key bit size values.

Threshold measurement

The value of the threshold is set as 500 for the generation of photons in order to measure the state of photon polarisation at Bob's side. It remains constant throughout the measurement and, hence, provides a '1' value so that the key generation bit is available with respect to the polarisation state received without error at the receiver side.

From Fig. 9, it is predictable that by setting the threshold value at Bob's side and during synchronization. Synchronization resulted in photons emitted to the detector with appropriate polarisation state at the receiver remaining 1 and others as 0. Values that are categorized as 0 get eliminated as it was the most significant bit and got eliminated simultaneously. Hence, an effective method of setting the threshold was analyzed and presented.

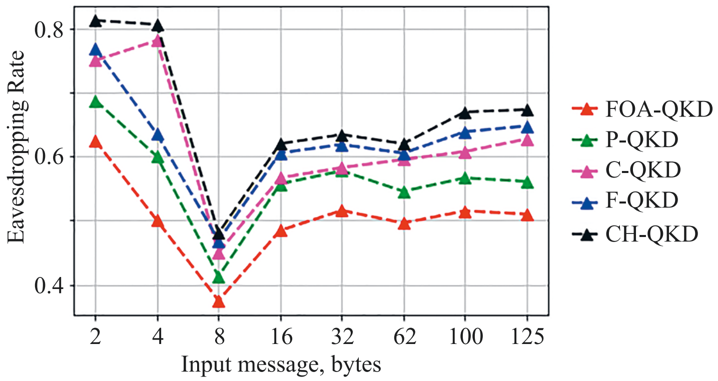

Fig. 7. Eve's dropping rate

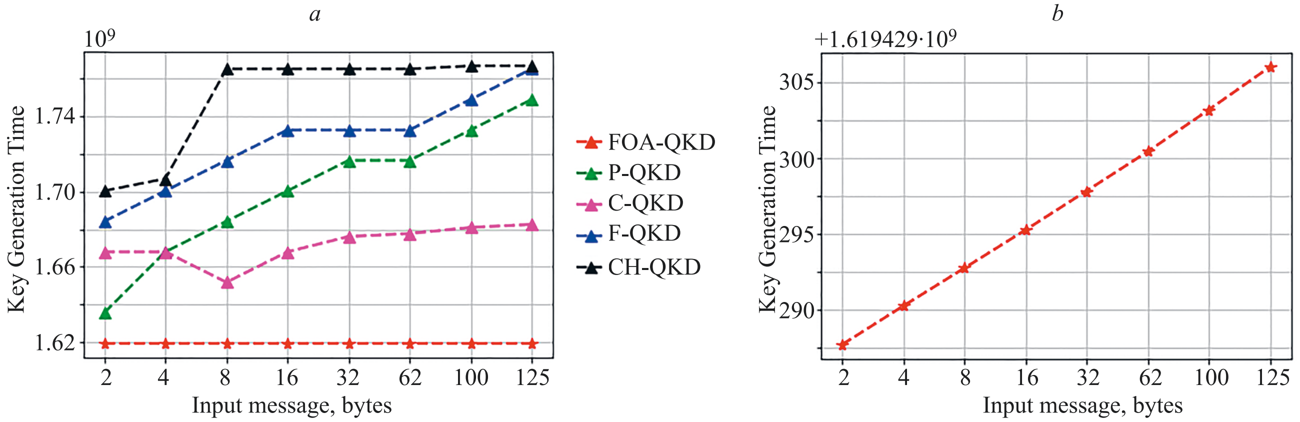

Fig. 8. Key generation rate comparative analysis (*a*); key generation rate for FOA-QKD protocol (*b*)

Table 3. Comparison among the proposed and existing techniques with performance metrics

Algorithm	Encryption time, ms	Decryption time, ms	Packet loss, %	Connection error, %
FOA-QKD	0.200	0.289	0.10	0.20
P-QKD	0.423	0.479	0.27	0.30
C-QKD	0.387	0.400	0.40	0.35
F-QKD	0.520	0.590	0.30	0.53

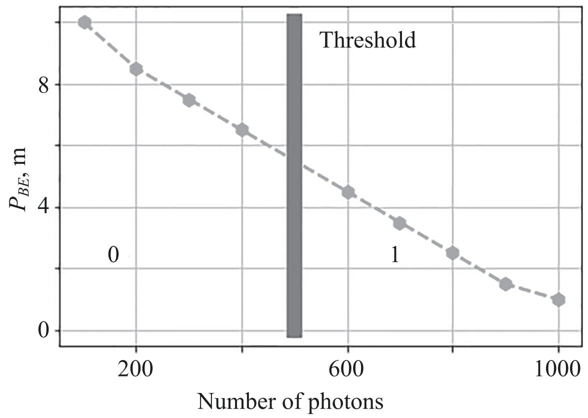

Fig. 9. Threshold rate analysis

Encryption and decryption time

The encryption and decryption times are shown in Table 3. It demonstrates that the proposed model takes less encryption and decryption times than other existing methods. The proposed FOA-QKD have an Encryption time of 0.2 ms and a Decryption time of 2.89 ms. The existing methods such as P-QKD, C-QKD and F-QKD have encryption time of 0.423 ms, 0.387 ms and 0.52 ms, as well as decryption time of 0.479 ms, 0.4 ms and 0.59 ms. The packet loss of the proposed model has 0.1 %, and the connection error is 0.2 %. This proves the proposed model performs better than existing techniques.

Conclusion

QKD protocol with improved key generation and distribution techniques for cloud users have been presented in this paper. Quantum mechanics of photon generation and its polarisation state measurement have been found useful at the end of secret communication model development. This method was widely used in satellite communication for secrecy maintenance. There were certain drawbacks of measuring receiver side bit sequence for generation of the raw key. This key generation was left unwillingly, taking much time and cost than by implementing a number of techniques that improved the complexity and cost of the model. Thus, an optimization scheme of FFA is implemented in this model to make it useful for selecting an appropriate block size that helps a conciliation strategy to achieve a fast key generation and helps a wide range of security with low cost as compared to others. Thus, the proposed model compares and predicts errors, eliminates them with respect to the threshold, generates key values and uses them for further transmission. Results were analyzed and compared with previous techniques, suggesting that the proposed model overcomes all those previous methods and performs efficiently.

References

1. Kiktenko E.O., Malyshev A.O., Gavreev M.A., Bozhedarov A.A., Pozhar N.O., Anufriev M.N., Fedorov A.K. Lightweight authentication for quantum key distribution. *IEEE Transactions on Information Theory*, 2020, vol. 66, no. 10, pp. 6354–6368. https://doi.org/10.1109/TIT.2020.2989459
2. Chitambar E., Fortescue B., Hsieh M.H. The conditional common information in classical and quantum secret key distillation. *IEEE Transactions on Information Theory*, 2018, vol. 64, no. 11, pp. 7381–7394. https://doi.org/10.1109/TIT.2018.2851564
3. Ji Z., Yeoh P.L., Zhang D., Chen G., Zhang Y., He Z., Yin H. Secret key generation for intelligent reflecting surface assisted wireless communication networks. *IEEE Transactions on Vehicular Technology*, 2021, vol. 70, no. 1, pp. 1030–1034. https://doi.org/10.1109/TVT.2020.3045728
4. Zhang W.R. From equilibrium-based business intelligence to information conservational quantum-fuzzy cryptography – a cellular transformation of bipolar fuzzy sets to quantum intelligence machinery. *IEEE Transactions on Fuzzy Systems*, 2018, vol. 26, no. 2, pp. 656–669. https://doi.org/10.1109/TFUZZ.2017.2687408
5. Koziel B., Azarderakhsh R., Kermani M.M., Jao D. Post-quantum cryptography on FPGA based on isogenies on elliptic curves. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 2017, vol. 64, no. 1, pp. 86–99. https://doi.org/10.1109/TCSI.2016.2611561
6. Yang Y.G., Xu P., Yang R., Zhou Y.H., Shi W.M. Quantum Hash function and its application to privacy amplification in quantum key distribution, pseudo-random number generation and image encryption. *Scientific Reports*, 2016, vol. 6, no. 1, pp. 19788. https://doi.org/10.1038/srep19788
7. Chen Z., Zhou K., Liao Q. Quantum identity authentication scheme of vehicular ad-hoc networks. *International Journal of Theoretical Physics*, 2019, vol. 58, no. 1, pp. 40–57. https://doi.org/10.1007/s10773-018-3908-y
8. Xu F., Curty M., Qi B., Lo H.K. Measurement-device-independent quantum cryptography. *IEEE Journal of Selected Topics in Quantum Electronics*, 2015, vol. 21, no. 3, pp. 148–158. https://doi.org/10.1109/JSTQE.2014.2381460
9. Dong T., Huang T. Neural cryptography based on complex-valued neural network. *IEEE Transactions on Neural Networks and Learning Systems*, 2020, vol. 31, no. 11, pp. 4999-5004. https://doi.org/10.1109/TNNLS.2019.2955165
10. Bai Z., Yang S., Li Y. High-efficiency reconciliation for continuous variable quantum key distribution. *Japanese Journal of Applied Physics*, 2017, vol. 56, no. 4, pp. 044401. https://doi.org/10.7567/JJAP.56.044401
11. Shang T., Chen R., Lei Q. Quantum random oracle model for quantum public-key encryption. *IEEE Access*, 2019, vol. 7, pp. 130024–130031. https://doi.org/10.1109/ACCESS.2019.2940406
12. Zoni D., Galimberti A., Fornaciari W. Efficient and scalable FPGA-oriented design of QC-LDPC bit-flipping decoders for post-quantum cryptography. *IEEE Access*, 2020, vol. 8, pp. 163419–163433. https://doi.org/10.1109/ACCESS.2020.3020262
13. Broadbent A., Schaffner C. Quantum cryptography beyond quantum key distribution. *Designs, Codes, and Cryptography*, 2016, vol. 78, no. 1, pp. 351–382. https://doi.org/10.1007/s10623-015-0157-4
14. Shenoy-Hejamadi A., Pathak A., Radhakrishna S. Quantum cryptography: key distribution and beyond. *Quanta*, 2017, vol. 6, no. 1, pp. 1–47. https://doi.org/10.12743/quanta.v6i1.57
15. Chan A.C. Distributed private key generation for identity based cryptosystems in ad hoc networks. *IEEE Wireless Communications Letters*, 2012, vol. 1, no. 1, pp. 46–48. https://doi.org/10.1109/WCL.2012.120211.110130
16. Jin R., Du X., Zeng K., Huang L., Xiao L., Xu J. Delay analysis of physical-layer key generation in dynamic roadside-to-vehicle networks. *IEEE Transactions on Vehicular Technology*, 2017, vol. 66, no. 3, pp. 2526–2535. https://doi.org/10.1109/TVT.2016.2582853
17. Wang J., Cheng L.M., Su T. Multivariate cryptography based on clipped hopfield neural network. *IEEE Transactions on Neural Networks and Learning Systems*, 2018, vol. 29, no. 2, pp. 353–363. https://doi.org/10.1109/TNNLS.2016.2626466
18. Xu P., Cumanan K., Ding Z., Dai X., Leung K.K. Group secret key generation in wireless networks: algorithms and rate optimization. *IEEE Transactions on Information Forensics and Security*, 2016, vol. 11, no. 8, pp. 1831–1846. https://doi.org/10.1109/TIFS.2016.2553643

Литература

1. Kiktenko E.O., Malyshev A.O., Gavreev M.A., Bozhedarov A.A., Pozhar N.O., Anufriev M.N., Fedorov A.K. Lightweight authentication for quantum key distribution // IEEE Transactions on Information Theory. 2020. V. 66. N 10. P. 6354–6368. https://doi.org/10.1109/TIT.2020.2989459
2. Chitambar E., Fortescue B., Hsieh M.H. The conditional common information in classical and quantum secret key distillation // IEEE Transactions on Information Theory. 2018. V. 64. N 11. P. 7381–7394. https://doi.org/10.1109/TIT.2018.2851564
3. Ji Z., Yeoh P.L., Zhang D., Chen G., Zhang Y., He Z., Yin H. Secret key generation for intelligent reflecting surface assisted wireless communication networks // IEEE Transactions on Vehicular Technology. 2021. V. 70. N 1. P. 1030–1034. https://doi.org/10.1109/TVT.2020.3045728
4. Zhang W.R. From equilibrium-based business intelligence to information conservational quantum-fuzzy cryptography – a cellular transformation of bipolar fuzzy sets to quantum intelligence machinery // IEEE Transactions on Fuzzy Systems. 2018. V. 26. N 2. P. 656–669. https://doi.org/10.1109/TFUZZ.2017.2687408
5. Koziel B., Azarderakhsh R., Kermani M.M., Jao D. Post-quantum cryptography on FPGA based on isogenies on elliptic curves // IEEE Transactions on Circuits and Systems I: Regular Papers. 2017. V. 64. N 1. P. 86–99. https://doi.org/10.1109/TCSI.2016.2611561
6. Yang Y.G., Xu P., Yang R., Zhou Y.H., Shi W.M. Quantum Hash function and its application to privacy amplification in quantum key distribution, pseudo-random number generation and image encryption // Scientific Reports. 2016. V. 6. N 1. P. 19788. https://doi.org/10.1038/srep19788
7. Chen Z., Zhou K., Liao Q. Quantum identity authentication scheme of vehicular ad-hoc networks // International Journal of Theoretical Physics. 2019. V. 58. N 1. P. 40–57. https://doi.org/10.1007/s10773-018-3908-y
8. Xu F., Curty M., Qi B., Lo H.K. Measurement-device-independent quantum cryptography // IEEE Journal of Selected Topics in Quantum Electronics. 2015. V. 21. N 3. P. 148–158. https://doi.org/10.1109/JSTQE.2014.2381460
9. Dong T., Huang T. Neural cryptography based on complex-valued neural network // IEEE Transactions on Neural Networks and Learning Systems. 2020. V. 31. N 11. P. 4999–5004. https://doi.org/10.1109/TNNLS.2019.2955165
10. Bai Z., Yang S., Li Y. High-efficiency reconciliation for continuous variable quantum key distribution // Japanese Journal of Applied Physics. 2017. V. 56. N 4. P. 044401. https://doi.org/10.7567/JJAP.56.044401
11. Shang T., Chen R., Lei Q. Quantum random oracle model for quantum public-key encryption // IEEE Access. 2019. V. 7. P. 130024–130031. https://doi.org/10.1109/ACCESS.2019.2940406
12. Zoni D., Galimberti A., Fornaciari W. Efficient and scalable FPGA-oriented design of QC-LDPC bit-flipping decoders for post-quantum cryptography // IEEE Access. 2020. V. 8. P. 163419–163433. https://doi.org/10.1109/ACCESS.2020.3020262
13. Broadbent A., Schaffner C. Quantum cryptography beyond quantum key distribution // Designs, Codes, and Cryptography. 2016. V. 78. N 1. P. 351–382. https://doi.org/10.1007/s10623-015-0157-4
14. Shenoy-Hejamadi A., Pathak A., Radhakrishna S. Quantum cryptography: key distribution and beyond // Quanta. 2017. V. 6. N 1. P. 1–47. https://doi.org/10.12743/quanta.v6i1.57
15. Chan A.C. Distributed private key generation for identity based cryptosystems in ad hoc networks // IEEE Wireless Communications Letters. 2012. V. 1. N 1. P. 46–48. https://doi.org/10.1109/WCL.2012.120211.110130
16. Jin R., Du X., Zeng K., Huang L., Xiao L., Xu J. Delay analysis of physical-layer key generation in dynamic roadside-to-vehicle networks // IEEE Transactions on Vehicular Technology. 2017. V. 66. N 3. P. 2526–2535. https://doi.org/10.1109/TVT.2016.2582853
17. Wang J., Cheng L.M., Su T. Multivariate cryptography based on clipped hopfield neural network // IEEE Transactions on Neural Networks and Learning Systems. 2018. V. 29. N 2. P. 353–363. https://doi.org/10.1109/TNNLS.2016.2626466
18. Xu P., Cumanan K., Ding Z., Dai X., Leung K.K. Group secret key generation in wireless networks: algorithms and rate optimization // IEEE Transactions on Information Forensics and Security. 2016. V. 11. N 8. P. 1831–1846. https://doi.org/10.1109/TIFS.2016.2553643

19. Howe J., Khalid A., Rafferty C., Regazzoni F., O’Neill M. On practical discrete Gaussian samplers for lattice-based cryptography. *IEEE Transactions on Computers*, 2018, vol. 67, no. 3, pp. 322–334. https://doi.org/10.1109/TC.2016.2642962
20. Dey S., Hossain A. Session-key establishment and authentication in a smart home network using public key cryptography. *IEEE Sensors Letters*, 2019, vol. 3, no. 4, pp. 8667393. https://doi.org/10.1109/LSENS.2019.2905020
21. Zhang J., He B., Duong T.Q. Woods R. On the key generation from correlated wireless channels. IEEE Communications Letters, 2017, vol. 21, no. 4, pp. 961–964. https://doi.org/10.1109/LCOMM.2017.2649496
22. He D., Zeadally S. An analysis of RFID authentication schemes for internet of things in healthcare environment using elliptic curve cryptography. *IEEE Internet of Things Journal*, 2015, vol. 2, no. 1, pp. 72–83. https://doi.org/10.1109/JIOT.2014.2360121
23. Furqan H.M., Hamamreh J.M., Arslan H. New Physical layer key generation dimensions: Subcarrier indices/positions-based key generation. *IEEE Communications Letters*, 2021, vol. 25, no. 1, pp. 59–63. https://doi.org/10.1109/LCOMM.2020.3025262
24. Almajed H.N., Almogren A.S. SE-ENC: A secure and efficient encoding scheme using elliptic curve cryptography. *IEEE Access*, 2019, vol. 7, pp. 175865–175878. https://doi.org/10.1109/ACCESS.2019.2957943

Authors

Mallavalli Raghavendra Suma — Assistant Professor, Dayananda Sagar College of Engineering, Bengaluru, 560078, India, https://orcid.org/0000-0002-2842-0942, sumamrvp@gmail.com

Perumal Madhumathy — PhD, Associate Professor, RV Institute of Technology and Management, Bengaluru, 560076, India, https://orcid.org/0000-0003-2803-3712, Madhumathyp.rvitm@rvei.edu.in

Received 09.08.2021
Approved after reviewing 11.01.2022
Accepted 31.01.2022

19. Howe J., Khalid A., Rafferty C., Regazzoni F., O’Neill M. On practical discrete Gaussian samplers for lattice-based cryptography // IEEE Transactions on Computers. 2018. V. 67. N 3. P. 322–334. https://doi.org/10.1109/TC.2016.2642962
20. Dey S., Hossain A. Session-key establishment and authentication in a smart home network using public key cryptography // IEEE Sensors Letters. 2019. V. 3. N 4. P. 8667393. https://doi.org/10.1109/LSENS.2019.2905020
21. Zhang J., He B., Duong T.Q. Woods R. On the key generation from correlated wireless channels // IEEE Communications Letters. 2017. V. 21. N 4. P. 961–964. https://doi.org/10.1109/LCOMM.2017.2649496
22. He D., Zeadally S. An analysis of RFID authentication schemes for internet of things in healthcare environment using elliptic curve cryptography // IEEE Internet of Things Journal. 2015. V. 2. N 1. P. 72–83. https://doi.org/10.1109/JIOT.2014.2360121
23. Furqan H.M., Hamamreh J.M., Arslan H. New Physical layer key generation dimensions: Subcarrier indices/positions-based key generation // IEEE Communications Letters. 2021. V. 25. N 1. P. 59–63. https://doi.org/10.1109/LCOMM.2020.3025262
24. Almajed H.N., Almogren A.S. SE-ENC: A secure and efficient encoding scheme using elliptic curve cryptography // IEEE Access. 2019. V. 7. P. 175865–175878. https://doi.org/10.1109/ACCESS.2019.2957943

Авторы

Сума Маллавалли Рагхавендра — доцент, Инженерный колледж Даянанда Сагар, Бангалор, 560078, Индия, https://orcid.org/0000-0002-2842-0942, sumamrvp@gmail.com

Мадхумати Перумал — доктор наук, доцент, RV Институт технологий и менеджмента, Бангалор, 560076, Индия, https://orcid.org/0000-0003-2803-3712, Madhumathyp.rvitm@rvei.edu.in

Статья поступила в редакцию 09.08.2021
Одобрена после рецензирования 11.01.2022
Принята к печати 31.01.2022