Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 4809210, 13 pages
https://doi.org/10.1155/2022/4809210

Research Article

QSLT: A Quantum-Based Lightweight Transmission Mechanism against Eavesdropping for IoT Networks

Gang Liu, Jingyuan Han, Yi Zhou, Tao Liu, and Jian Chen

China Telecom Research Institute, Shanghai, China

Correspondence should be addressed to Gang Liu; liug8@chinatelecom.cn

Received 21 April 2022; Revised 16 August 2022; Accepted 1 September 2022; Published 27 September 2022

Academic Editor: Rüdiger Pryss

Copyright © 2022 Gang Liu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Quantum Key Distribution (QKD) is a promising paradigm for Internet of Things (IoT) networks against eavesdropping attacks. However, classical quantum-based mechanisms are overweight and expensive for resource-constrained IoT devices. That is, the devices need to frequently exchange with the QKD controller via an out-band quantum channel. In this paper, we propose a novel Quantum-based Secure and Lightweight Transmission (QSLT) mechanism to ease the overweight pain for IoT devices against eavesdropping. Particularly, the mechanism predistributes quantum keys into IoT devices with SIM cards. Using one of the keys, QSLT encrypts or decrypts IoT sensitive data. It is noting that an in-band key-selection method is used to negotiate the session key between two different devices. For example, on one IoT device, the in-band method inserts a key-selection field at the end of the encrypted data to indicate the key's sequence number. After another device receives the data, QSLT extracts the key-selection field and decrypts the data with the selected quantum key stored locally. We implement the proposed mechanism and evaluate its security and transmission performances. Experimental results show that QSLT can transmit IoT data with a lower delay while guaranteeing the security performance. Besides, QSLT also decreases power usage by approximately 58.77% compared with state of the art mechanisms.

1. Introduction

Internet of Things (IoT) booms with the development of smart homes, cities, and factories [1, 2]. International Data Corporation (IDC) predicts that there will be 41.6 billion IoT devices in 2025 [3]. With this increment, oceans of data (79.4 zettabytes predicted by IDC) will be generated from actuators, sensors, vehicles, and other IoT devices [4]. This massive amount of data brings a secure transmission challenge for IoT networks [5]. For example, attackers could eavesdrop on transmission channels established between different IoT devices, intercept the traffic data, and steal sensitive information with brute-force cracking [6, 7].

Various mechanisms have been proposed to deal with the transmission challenge [8–10]. Particularly, a long and complicated encryption key can be used to increase difficulties of eavesdropping for the IoT systems [11]. Besides, a programmable network immune mechanism, which is equipped with three lines of defenses, is proposed to provide a softwarized network immunity against the intractable eavesdropping [12]. These encryption-based mechanisms are powerful, but they could be bypassed by the advances in computation capabilities [13]. That is, cryptographic-based secure transmission mechanisms are powerful but never total.

Quantum mechanics provides a new research direction for transmitting IoT data securely against eavesdropping attacks [14–16]. For example, a novel eavesdropping defense mechanism to transmit the data between IoT devices with Quantum Key Distribution (QKD) [17]. Besides, a QKD-enhanced IoT architecture is designed and provides a key provisioning mechanism to ensure the security of data transmission [18]. However, state of the art quantum-based mechanisms are not applicable for IoT devices due to two drawbacks: (1) the mechanisms increase the overhead burden for IoT devices because the devices frequently exchange with QKD controller via an out-band channel. (2) It is expensive to establish quantum channels between IoT devices [19].

To deal with the drawbacks above, this paper introduces a quantum IoT framework and proposes a novel Quantum-based Secure and Lightweight Transmission (QSLT) mechanism for IoT networks against eavesdropping attacks. Particularly, QSLT first predistributes quantum keys into IoT devices. Then, QSLT chooses one quantum key to encrypt IoT data and 'tells' other devices the key's sequence number via an in-band key-selection method. The in-band method inserts a key-selection field at the end of the encrypted data to indicate the key's sequence number. Finally, QSLT extracts the key-selection field after receiving the data and decrypts the data with the selected key stored locally on IoT devices. The main contributions of this paper can be summarized as follows:

(1) This paper detailly introduces a quantum-based IoT framework to ensure secured IoT data transmission, processing, and sharing. The framework comprehensively includes four classical quantum applications in IoT domain: QKD, quantum secret sharing, quantum communication, and quantum signature

(2) This paper novelly proposes a quantum-based secure and lightweight transmission mechanism for IoT networks against eavesdropping attacks. The mechanism can encrypt or decrypt IoT data by using quantum keys without a centralized QKD controller and decreases the communication overhead for IoT devices

(3) This paper implements the QSLT and conducts experiments in our data center rooms. Experimental results show that QSLT can transmit IoT data with a lower delay while guaranteeing the security performance. Besides, QSLT also decreases the power usage by ~58.77% compared with QKD-based mechanisms

The remainder of this paper is organized as follows. Section II presents related works. Section III introduces the quantum-based IoT framework in detail. Section IV introduces the principle of QSLT mechanism. Section V evaluates the security and transmission performances of QSLT mechanism. Section VI discusses the limitations of QSLT mechanism. Section VII concludes this paper.

2. Related Works

It is a long 'war' between IoT devices and eavesdroppers. Traditionally, IoT data is encrypted by various cryptographic mechanisms against eavesdropping attacks. For example, a novel key management mechanism is presented to encrypt the secret data against eavesdropping in wireless links [20]. The mechanism encrypts secret data with the randomness characteristics of wireless channels, i.e., according to instantaneous channel gain between a sensor and an ally fusion center. The location-based properties of wireless channels enable the sensor and ally fusion center to share keys secretly, which are difficult for eavesdroppers to intercept. Experimental results show that the proposed mechanism outperforms other mechanisms over a broad range of signal-to-noise-ratio values without compromising the security goals—perfect secrecy. An encoding scheme, i.e., encrypting the packet header and trailer information, is proposed to use service-oriented routers for providing secure data transmission against eavesdropping attacks [21]. The experimental results demonstrate that the average delays of encrypting total combined packets are with range from 180.14μs to 235.48μs using various cryptographic algorithms. Besides, an enhancing Internet Protocol Security (IPsec) mechanism is presented to mitigate eavesdropping attacks [22]. An IPsec-based scheme is proposed to secure the software-defined mobile network communication [23]. Moreover, a lightweight in-network anonymity solution is proposed against eavesdropping within the memory and processing constraints of hardware switches [24]. The solution conceals IP addresses in packet headers to hide the addresses from the destination server without requiring terminal modification or cooperation from networks. The solution is implemented on the Barefoot Tofino switch and can protect user identity against public domain name system and other services.

Recently, quantum mechanics have attracted many researches to power IoT networks. For example, a new authentication and encryption protocol based on quantum walks are proposed to build a blockchain framework for secure data transmission [25]. Instead of using classical cryptographic hash functions, the proposed protocol uses quantum hash functions to help IoT devices to effectively share their data and full control of their records. The analysis results show that the proposed protocol can effectively defend against impersonation and eavesdropping attacks. A novel quantum swarm optimization algorithm is proposed for IoT deployments to provide enhanced connectivity, reduced energy consumption, and optimized delay [26]. The algorithm uses multiple inputs from heterogeneous IoT using a hybrid approach based on quantum and bioinspired optimization techniques for optimal routing. The experimental results demonstrate that the proposed algorithm costs a minimum of 30.30% lesser energy and improves the throughput by a minimum of 29.87%. A quantum cryptography mechanism is proposed to secure IoT-based healthcare systems [27]. The mechanism uses quantum cryptography to encrypt patient's privacy data against various attacks. Besides, image-encryption mechanisms are proposed using quantum mechanics for privacy-preserving medical images in IoT domain [15, 28]. The mechanisms use the features of quantum walk to construct a new s-box method, which plays a significant role in block cipher techniques. Based on this, the mechanisms have a novel encryption strategy for secure transmission of sensitive medical images. The experimental results show that the proposed mechanisms have better security properties and efficacy in terms of cryptographic performance. To mitigate security breaches of classical cryptographic algorithms in the era of quantum computing, quantum cryptographic algorithms are introduced in terms of the pros and cons of implementing quantum cryptography for IoT security [29]. Moreover, a quantum-powered algorithm is proposed to detect attackers between a IoT transmitter and IoT receiver by using machine learning techniques [30]. The algorithm combines artificial neural network and deep learning techniques to detect the presence of an attacker without disrupting quantum key distribution process. The results show that the proposed algorithm can effectively detect attackers with an accuracy of 99%.

To defend eavesdropping attacks, various quantum-based mechanisms have been proposed for IoT networks. For example, a novel communication authentication mechanism with QKD technology is proposed for RFID system against eavesdropping attacks [31]. The proposed mechanism distributes quantum keys to the RFID tags and readers via weakly coherent photons transmitted through optical fiber. The proposed mechanism also includes the RFID system's initialization, the transmission, reception, and acquisition of random quantum keys. The analysis results prove that the proposed mechanism can mitigate eavesdropping attacks with solid security. A software-defined IoT and optical fiber QKD are integrated to realize the selection of quantum keys for IoT devices [32]. The software-defined IoT network with fiber-based QKD can provide IoT devices with quantum keys to enhance their battery lifetime, i.e., serve a significant number of IoT devices with the same level of security while drastically improving energy savings for the IoT infrastructure. The experimental results demonstrate that the proposed scheme saves an 18% energy efficiency compared with the standard key generation scheme. Besides, a secure transmission mechanism is proposed to secure the communication between smart grid users and servers through QKD technology [33]. The proposed mechanism achieves a mutual authentication between smart grid users and servers and provides solid security against eavesdropping attacks by generating secret quantum keys which consist of qubits. The verification results show that the proposed mechanism works well in the presence of an eavesdropper. Moreover, a QKD-enhanced IoT architecture is designed and provides a key provisioning mechanism to ensure the security of data transmission [17, 18]. The key provisioning mechanism is residual-adaptive and can efficiently utilize the quantum key resources. Simulation results show that the performance of key distribution success rate is highly influenced by factors such as the capacity of each quantum node pair and key generation rate of access nodes, as well as key requirement of services. In general, these mechanisms are novel but not applicable for IoT devices, because they increase the burden and the cost of establishing quantum channels.

3. Quantum-Based IoT Framework

This section introduces a preliminary quantum-backed IoT network framework. As shown in Figure 1, quantum applications have been equipped into the IoT network in terms of the smart house, the industry 4.0, the high-speed rail, and other IoT scenarios. Particularly, the IoT network includes various nodes such as quantum servers, satellites, phones, routers, and smart watches. It is noting that quantum servers could connect to other nodes via quantum and classical channels. To the best of our knowledge, the quantum channel is very little in the current network. The quantum applications typically involve four parts: QKD, quantum secret sharing, quantum communication, and quantum signature. The detail of each part is introduced in the following paragraphs.

QKD is a secure mechanism for sharing and exchanging secret quantum keys that are necessary for cryptographic protocols. Typically, if an eavesdropper steals cryptography keys, the eavesdropper will be detected by the communicators with appropriate quantum mechanics. There are various use-cases for QKD in IoT domain. For example, a novel RFID communication authentication protocol is proposed for sensors to mitigate eavesdropping attacks [31]. A provision mechanism of quantum keys is proposed to save the battery usage for IoT devices [32]. A smart grid authentication mechanism is proposed to provide secure data transmission between users and servers by using quantum keys [33].

Quantum Secret Sharing (QSS) is a procedure for splitting a message into several parts so that multiparties could share the message securely. The quantum keys in QSS are very useful to create private keys for every party, such that the message could only be retrieved through the cooperation of all parties. Typically, in a three-party QSS system, a party named Alice sends private parts to two other parties named Bob and Charlie, separately. In this way, Bob and Charlie can get the complete message only if they bring their private parts together. There are various use-cases for QSS in IoT domain. For example, a novel quantum steganography protocol is proposed in fog and mobile edge computing [34].

Quantum Communication (QC) is a new communication technology that directly transmits secret information via quantum channels without setting any cryptography keys. Typically, QC only requires a single quantum channel and natively prevents eavesdropping attacks with quantum mechanics. There are various use-cases for QC in IoT domain. For example, a quantum secure data transfer mechanism is proposed by using pulse shape-encoded optical qubits [35]. A quantum tunneling RFID tag is designed to minimize battery waste of IoT devices and improve the range of backscattering systems [36].

Quantum Signature (QS) is a quantum mechanical equivalent of a digital signature on a paper document. QS can provide a secure method of signing messages so that the signer can neither deny the messages nor forge recipients or possible attackers of the messages. Typically, classical signature mechanisms depend on computational complexity assumptions, and QS is a better alternative mechanism because it can provide native unconditional security. There are various use-cases for QS in IoT domain. For example, an arbitrated quantum signature mechanism with cluster states [37] and a multiproxy strong blind quantum signature mechanism [38].

This paper focuses on designing a quantum-based secure and lightweight transmission mechanism for IoT networks. To the best of our knowledge, quantum channels are very

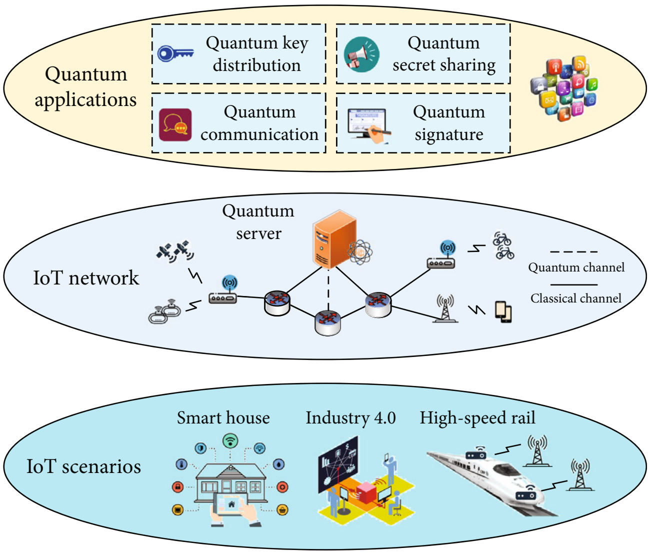


Figure 1: The quantum-based IoT framework.

few in the current network, and it is very expensive for IoT devices (e.g., sensors) to establish quantum channels. Therefore, how to generate and distribute quantum keys for resource-constrained devices is introduced in the following paragraphs. Besides, a secure and lightweight transmission mechanism is also proposed in this paper so that IoT devices could transmit sensitive data securely and effectively.

4. QSLT Principle

This section introduces the principle of QSLT mechanism. First, the quantum random number is theoretically analyzed to provide a fundamental theory for quantum keys. Second, how to generate quantum keys with the quantum random number is introduced in detail. Finally, the secure transmission algorithm and lightweight transmission policy are introduced for IoT networks against eavesdropping attacks.

4.1. The Quantum Random Number. This paper introduces Quantum Random Number Generators (QRNGs) which are truly random compared with Pseudo Random Number Generators (PRNGs). The reason of using a truly random number is that randomness affects the security performance of cryptography keys. Typically, PRNGs are computer algorithms designed to simulate randomness and are reversible in the sense that the results of computer algorithms could be predictable. QRNGs are based on the inherent randomness in quantum mechanics (e.g., the radioactive decay of an atom or the detection of a photon having passed through a beam splitter) and are strongly irreversible due to quantum physical attributes. Quantum mechanics are out of the scope of this paper. The details can be found in [39].

QRNGs are highly relevant to the basis state of a qubit (quantum bit). Particularly, the classic quantum basis state can be represented using a 2-dimensional system. For example, the basis states can be denoted as $|0\rangle$ and $|1\rangle$ with a Bloch sphere (which is a 2-dimensional system). By inputting these basis states, a logical gate of quantum computers can classify qubits into logical 0 and 1. To get QRNGs, the following state is prepared in a quantum computer:

$$|\varphi\rangle = \frac{1}{\sqrt{2}}\left|0\right\rangle + \frac{1}{\sqrt{2}}\left|1\right\rangle. \tag{1}$$

There is a 50% chance to measure the aforementioned state as 0, and vice versa. By continually repeating the measurement, we can get as many truly random bits as required. This paper adopts the truly random numbers for generating quantum keys to transmit data securely in IoT networks. The generation details can be found in the following subsection.

4.2. The Generation of Quantum Keys. By using the QRNGs, this paper generates quantum keys to encrypt IoT sensitive data. Particularly, a 128-bit random string is first generated by the QRNGs and is denoted as $S_1, S_2, \cdots S_N$, $N = 16$. Then, a subkey can be generated by using the following equations:

$$\left\{\begin{matrix} W_1 \\ W_2 \\ W_3 \\ W_4 \end{matrix}\right\} = \left\{\begin{matrix} S_1 & S_5 & S_9 & S_{13} \\ S_2 & S_6 & S_{10} & S_{14} \\ S_3 & S_7 & S_{11} & S_{15} \\ S_4 & S_8 & S_{12} & S_{16} \end{matrix}\right\},$$

$$s_{key} = \{W_i \oplus W_{i+1}, W_{i+1} \oplus W_{i+2}, W_{i+2} \cdots \cdots \oplus W_{i+3}, G(W_{i+4} \oplus W_i) \mid i = 1, 2, 3, 4\}, \tag{2}$$

whereas $\{W_i \mid i = 1, 2, 3, 4\}$ is a set of 8-bit random strings, s_{key} represents the subkey, $G(\bullet)$ denotes a function that reverses and replaces the 8-bit random strings. Finally, the quantum key can be generated by combining all the subkeys which can be denoted as:

$$key = \left\{s_{key_j} \mid j = 1, 2, \cdots, 11\right\}. \tag{3}$$

It is noting that the generated quantum keys are predistributed into SIM cards, because quantum communication channels are not integrated in this paper. A quantum key distribution mechanism will be proposed in the future when the quantum communication channels are equipped. Typically, a SIM card (as shown in Figure 2) includes four parts: CPU, ROM, RAM, and EEPROM. The CPU part performs basic logic and control instructions. The ROM part is a type of nonvolatile memory used in electronic devices. The RAM part is typically used to store working data and machine code. Besides, the EEPROM part stores quantum keys that are used to encrypt sensitive data transmitted between IoT devices.

4.3. The Secure Transmission Algorithm. By using the aforementioned quantum keys, this paper introduces a secure algorithm to encrypt IoT sensitive data. Particularly, there are four steps to transform the plaintext of IoT data into a ciphertext. Step 1 adds a plaintext and a quantum key. The length of each plaintext is 128-bit length. If the length is larger than 128-bit, then the plaintext will be cut into multiple substrings. Step 2 maps the result of step 1 with an s-box matrix. The s-box matrix can be generated by using the following equations:

$$\begin{gathered}\{(x-1)(y-1)\} \xrightarrow{GF(2^8)} \left\{(x-1)'(y-1)'\right\}, \\ b_i{}' = b_i \oplus b_{(i+4) \bmod 8} \oplus b_{(i+5) \bmod 8} \\ \oplus\, b_{(i+6) \bmod 8} \oplus b_{(i+7) \bmod 8} \oplus c_i \end{gathered}, \tag{4}$$

whereas $\{x-1\}\{y-1\}$ represents the x_{th} row and y_{th} column element in the s-box matrix. $GF(2^8)$ is a finite field and it has 256 elements. Besides, b_i and c_i denote the i_{th} bit of a byte element. Step 3 executes a left shift operation with the result of step 2. Step 4 gets the result of step 3 and mixes each column of the result in the finite field $GF(2^8)$. Step 5 repeats step 1-4 for 10 times and gets the ciphertext of IoT data. Algorithm 1 shows the pseudocode of encrypting IoT data from a plaintext into a ciphertext.

4.4. The Lightweight Transmission Policy. To ease the overhead burden for IoT networks, this paper promotes the quantum-based transmission mechanism in terms of lightweight performance. Particularly, quantum-based transmission mechanisms have a centralized controller to select cryptography keys for IoT nodes and increase the overhead burden for IoT nodes, because the nodes have frequent out-band communication exchanges with the controller. Therefore, the QSLT mechanism introduces an in-band key-selection method for IoT nodes. As shown in Figure 3, the in-band method inserts a key-selection field into traffic packets on the IoT node N1, transmits the packets to the IoT node N2, and extracts the key-selection field on the IoT node N2. After IoT nodes N1 and N2 finish the key-selection process, both the nodes 'know' how to encrypt/decrypt transmission data for IoT networks. The proposed mechanism is lightweight for IoT nodes and without an extra out-band control channel.

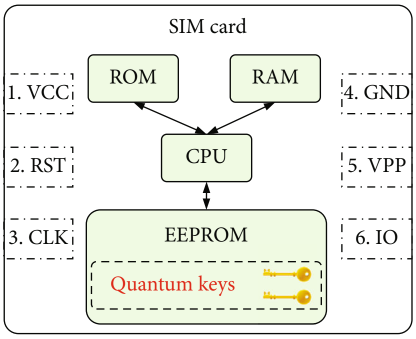


Figure 2: The SIM card block diagram.

Figure 4 depicts the workflows of the lightweight transmission mechanism. There are three steps: (1) the IoT node N1 selects a quantum key from its local SIM card; (2) the IoT node N1 encrypts a traffic packet and inserts a key-selection field; and (3) the IoT node N2 receives the packet, extracts the key-selection field, and decrypts the packet with the selected quantum key. It is noting that whereof the packet to insert the key-selection field is different for various IoT network protocols. For example, the Type of Service field for IPv4 protocol, the Next Header field for IPv6 protocol, and the variable length header field for MQTT protocol. As shown in Figure 4, the lightweight transmission mechanism is in-band and saves communication exchanges compared with out-band key-selection method. That is, the proposed mechanism is more lightweight for IoT nodes.

5. Performance Evaluation

This section evaluates the performance of QSLT mechanism in our data center rooms. We conduct a series of experiments to evaluate the security and transmission performances. The security performance is evaluated by using NIST-800-22 tests [40] and machine learning model tests [41]. The NIST-800-22 is a statistical test suite for evaluating the randomness of cryptographic keys. The transmission performance is evaluated by measuring the transmission delay and power usage. For comparison, state of the art mechanisms are also implemented in our experiments as the baseline mechanisms. To ensure a fair comparison, both the proposed and baseline mechanisms have the same experimental parameters, e.g., CPU and RAM resources. Besides, each experiment is repeated many times to eliminate the effect of uncontrollable environmental factors, e.g., temperature and humidity variations.

"#1-#15" denotes the NIST-800-22 test name listed in Table 1. "QSLT-1 K" denotes that generating a 1 Kbytes key using QLST mechanism and so on. "Baseline-1 K": denotes that generating a 1 Kbytes key using the baseline mechanism and so on.

5.1. The Security Performance. To evaluate the security performance of QSLT mechanism, this paper experimentally tests the randomness of cryptography keys. There are two reasons for evaluating the randomness of cryptography keys: (1) the security performance is difficult to quantize; and (2)

```
Input: $P_{\mathrm{IoT}}$ (plaintext data) and $Q_K$ (quantum keys)
Output: $C_{\mathrm{IoT}}$ (ciphertext data)
1 if length($P_{\mathrm{IoT}}$) > 128 then
2     $P_{\mathrm{IoT}}$.multi_string($\{\mathrm{sub}_{1P_{\mathrm{IoT}}}, \cdots, \mathrm{sub}_{NP_{\mathrm{IoT}}}\}$);
3 else
4     $R1 = P_{\mathrm{IoT}} \bmod Q_K$;
5 end
6 $R2 = \mathrm{map}(R1, s-\mathrm{box})$;
7 $R3 = \mathrm{left\_shift}(R2(:, N), 1\,\mathrm{byte})$;
8 $C_{\mathrm{IoT}} = \mathrm{mix\_col}(R3)$;
9 for $i \longleftarrow 1$ to 10 do
10     Repeat(lines(1, 8));
11 end
```

Algorithm 1: Encrypt IoT data with quantum keys.

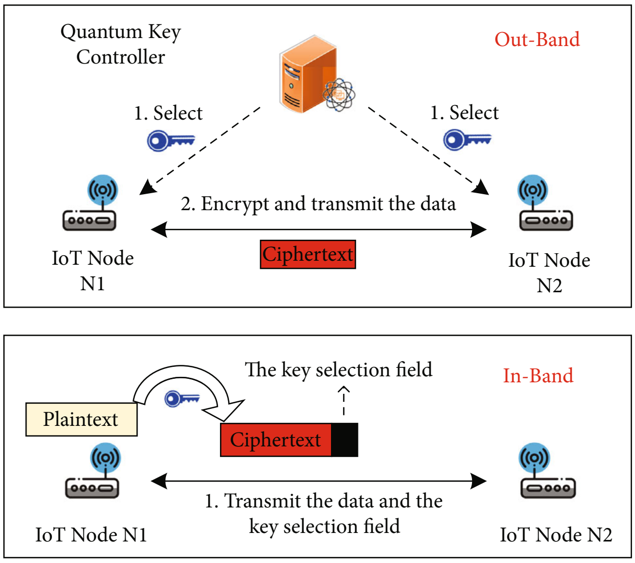


Figure 3: The lightweight policy against eavesdropping.

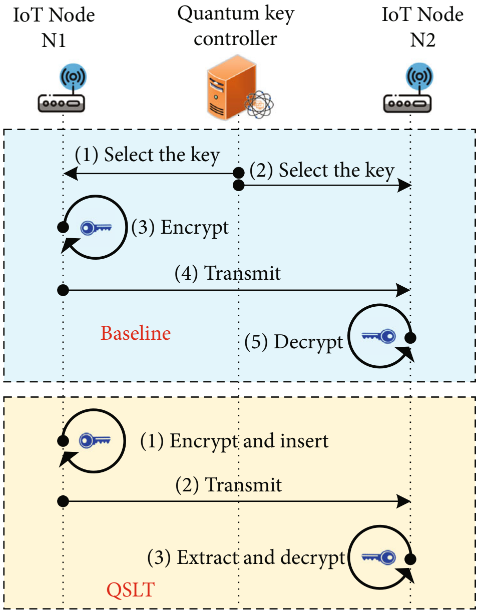


Figure 4: The workflows of QSLT and baseline mechanisms.

the security performance is very relevant to the key randomness [42]. Typically, QSLT and traditional symmetric/asymmetric cryptography mechanisms have keys generated by QRNGs and PRNGs, separately. Therefore, this paper takes PRNGs as a baseline for comparing the security performance with the QSLT. Besides, there are two classical methods to evaluate the randomness of QRNGs and PRNGs: NIST-800-22 tests [40] and machine learning models [41].

5.1.1. NIST-800-22 Tests. The NIST-800-22 test suites are standard suites of statistical tests. Particularly, there are 15 independent tests to evaluate the performance of QSLT and the baseline mechanisms. As shown in Table 1, the monobit test is the proportion of ones and zeroes for the entire sequence, its purpose is to determine whether the number of ones and zeros in a sequence is approximately 50%-50% chance. The frequency test within a block is the proportion of ones within M-bit blocks, its purpose is to determine whether the frequency of ones in an M-bit block is approximately M/2. The runs test is the total number of runs in the sequence, where a run is an uninterrupted sequence of identical bits. Besides, each test has a quantized metric (P value) whose detail is listed in Table 1.

In our experiments, the quantum random number of QSLT is generated by using the IBM quantum platform [43], and the pseudo random number of baseline mechanism is generated by using a Mersenne Twister algorithm [44]. The algorithm can generate uniform pseudorandom numbers and provides a super astronomical period of $2^{19937} - 1$ and 623-dimensional equidistribution up to 32-bit accuracy, while using a working area of only 624 words. The Mersenne Twister algorithm is selected as a baseline in this paper because the algorithm is popular and classical for generating uniform pseudorandom numbers. It is noting that any other variant of the algorithm can also be an alternative of general baseline. Besides, both the quantum and pseudo random numbers are evaluated by using the NIST-800-22 tests listed in Table 1. For comparison, both QSLT and the baseline mechanisms generate 1 K-, 5 K-, and 25 K-bits sequences, separately. All the source codes can be found via GitHub (The codes can be found via: https://github.com/KB00100100/paper-QSLT). The experimental results are shown in Table 2, in which the P value is computed by a series of statistics rules. Typically, a high P value could indicant a better randomness for the QSLT and baseline mechanisms.

As shown in Table 2, QSLT mechanism has a better performance in terms of 1 K-, 5 K-, and 25 K-bits sequences. Particularly, regarding 1 K-bits sequence, the #2, #3, #4, #6, #13, and #15 experimental results of QSLT are 0.69, 0.56, 0.48, 0.67, 0.11, and 0.15, separately. Both of the values are larger than the P values of baseline mechanism, that is, QSLT is more random than the baseline mechanism. Regarding the 5 K-bits sequence, QSLT has larger P values than the baseline mechanism. Regarding 25 K-bits sequence, the #2, #4, #5, #11, #14, and #15 experimental results of

Table 1: The NIST-800-22 tests.

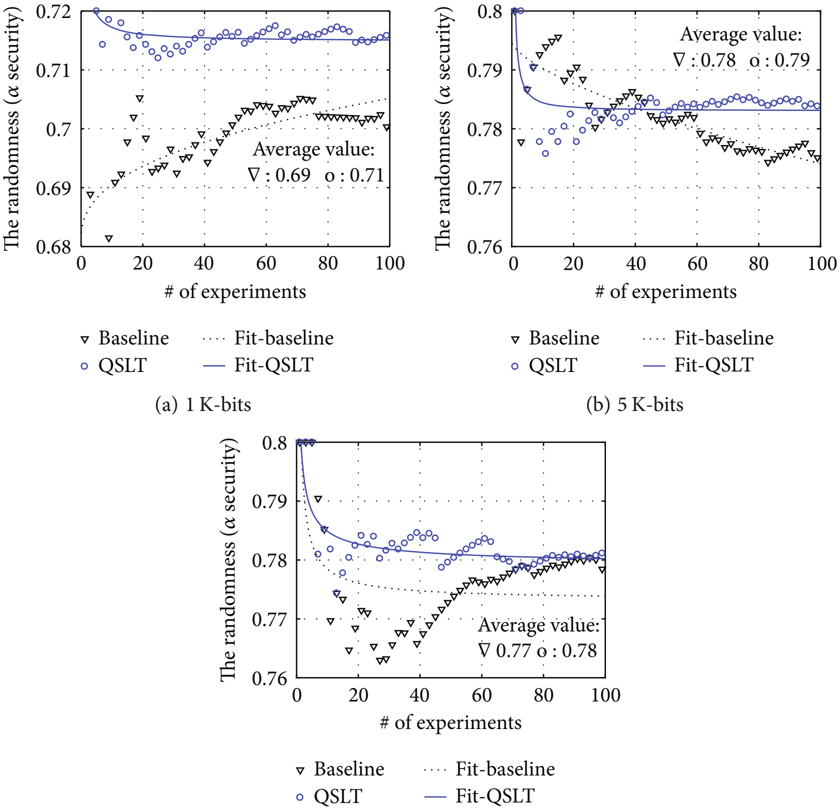
—	Test name	*P* value	Accept *P* value
1	Monobit	$\operatorname{erfc}\left(\frac{S_{\text{obs}}}{\sqrt{2}}\right)$	>0.01
2	Frequency	$\operatorname{igamc}\left(\frac{N}{2}, \frac{\chi^2(\text{obs})}{2}\right)$	>0.01
3	Runs	$\operatorname{erfc}\left(\frac{\lvert V_n(\text{obs}) - 2n\pi(1-\pi)\rvert}{2\sqrt{2n}\pi(1-\pi)}\right)$	>0.01
4	Longest run	$\operatorname{igamc}\left(\frac{K}{2}, \frac{\chi^2(\text{obs})}{2}\right)$	>0.01
5	Binary matrix rank	$e^{-\chi^2(\text{obs})/2}$	>0.01
6	Discrete Fourier transform	$\operatorname{erfc}\left(\frac{\lvert d\rvert}{\sqrt{2}}\right)$	>0.01
7	Nonoverlapping template matching	$\operatorname{igamc}\left(\frac{N}{2}, \frac{\chi^2(\text{obs})}{2}\right)$	>0.01
8	Overlapping template matching	$\operatorname{igamc}\left(\frac{5}{2}, \frac{\chi^2(\text{obs})}{2}\right)$	>0.01
9	Maurer's universal statistical	$\operatorname{erfc}\left(\left\lvert\frac{f_n - \text{expectedValue}(L)}{\sqrt{2}\sigma}\right\rvert\right)$	>0.01
10	Linear complexity	$\operatorname{igamc}\left(\frac{K}{2}, \frac{\chi^2(\text{obs})}{2}\right)$	>0.01
11	Serial	$\operatorname{igamc}\left(2^{m-2}, \nabla\psi_m^2\right)$ $\operatorname{igamc}\left(2^{m-3}, \nabla^2\psi_m^2\right)$	>0.01
12	Approximate entropy	$\operatorname{igamc}\left(2^{m-1}, \frac{\chi^2}{2}\right)$	>0.01
13	Cumulative sums	$\sum_{k=((-n/4z)+(1/4))}^{((n/4z)-(1/4))}\left[\Phi\left(\frac{(4k+1)z}{\sqrt{n}}\right) - \Phi\left(\frac{(4k-1)z}{\sqrt{n}}\right)\right]$	>0.01
14	Random excursions	$\operatorname{igamc}\left(\frac{5}{2}, \frac{\chi^2(\text{obs})}{2}\right)$	>0.01
15	Random excursions variant	$\operatorname{erfc}\left(\frac{\lvert\xi(x) - J\rvert}{\sqrt{2J(4\lvert\text{x}\rvert - 2)}}\right)$	>0.01

Table 2: The NIST-800-22 test results.

Mechanism							Test name *P* value						
	#1	#2	#3	#4	#5	#6	#7	#8-10	#11	#12	#13	#14	#15
QSLT-1K	0.10	0.69↑	0.56↑	0.48↑	—	0.67↑	0.99	—	0.06	0.08	0.11↑	—	0.15↑
Baseline-1K	0.77↑	0.23	0.44	0.34	—	0.63	0.99	—	0.46↑	0.63↑	0.09	0.36↑	—
QSLT-5K	0.84↑	0.61↑	0.73↑	0.63↑	0.85↑	0.65↑	1.00↑	—	0.26↑	0.67↑	0.67↑	0.01↑	0.01↑
Baseline-5K	0.73	0.37	0.69	0.34	0.74	0.10	0.99	—	0.19	0.37	0.43	—	—
QSLT-25K	0.11	0.20↑	0.59	0.50↑	0.54↑	0.24	0.99	—	0.39↑	0.38	0.06	0.08↑	0.05↑
Baseline-25K	0.20↑	0.04	0.79↑	0.34	0.45	0.50↑	0.99	—	0.26	0.50↑	0.17↑	—	0.01

QSLT are 0.20, 0.50, 0.54, 0.39, 0.08, and 0.05, separately. Both of the values are larger than *P* values of baseline mechanism. Therefore, we could conclude that QSLT is more random than the baseline mechanism, that is, QSLT is more secure for transmitting IoT data compared with the baseline mechanism.

To intuitively evaluate whether QSLT mechanism is more secure, this paper compares the randomness pass ratio



(a) 1 K-bits

(b) 5 K-bits

(c) 25 K-bits

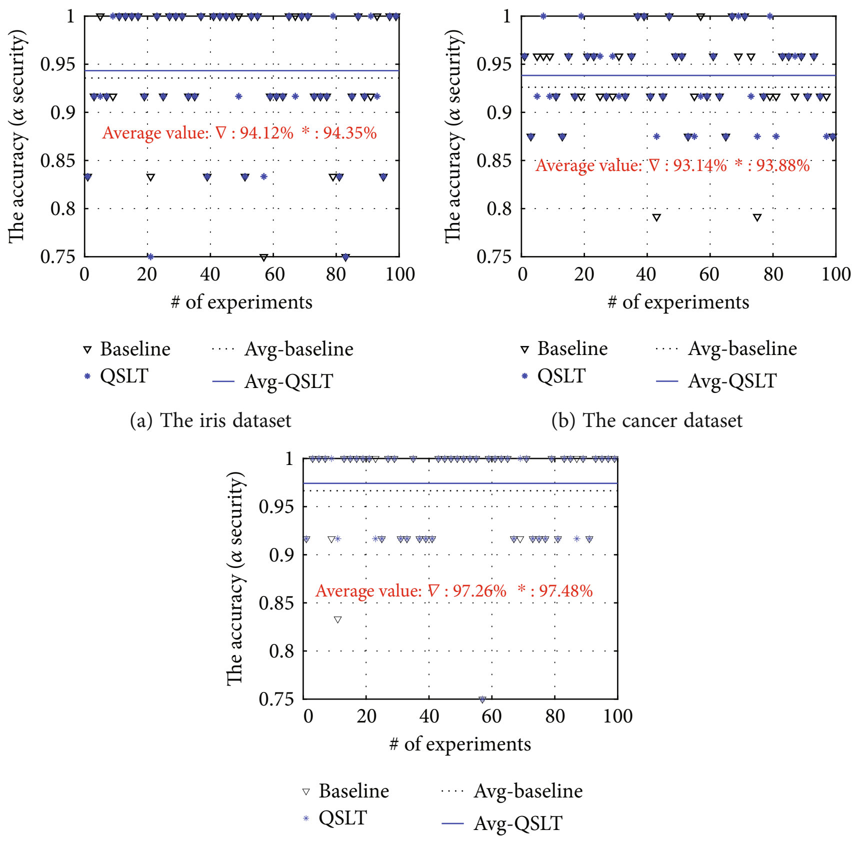
Figure 5: The security results of NIST-800-22 tests.

within QSLT and the baseline mechanisms. Particularly, the pass ratio represents the number of passed tests among all NIST-800-22 tests, it can be achieved by dividing the number of passed tests by 15. In our experiments, both QSLT and the baseline mechanisms generate 100 random sequences whose lengths are 1 K-, 5 K-, and 25 K-bits, separately. For each random sequence, this paper performs all NIST-800-22 tests, computes the pass ratio, and compares the pass ratio between QSLT and the baseline mechanisms. It is noting that a larger pass ratio means the tested sequence is more random, that is, it is more secure to use that sequence as a cryptography key.

The experimental results are shown in Figure 5. As shown in Figure 5(a), the pass ratio is fluctuant from 0.68 to 0.72, and the average value of QSLT and the baseline mechanisms are 0.71 and 0.69, separately. It is obvious that QSLT has a higher pass ratio than the baseline mechanism, that is, QSLT mechanism is more secure to generate a cryptography key. As shown in Figure 5(b), the pass ratio is fluctuant from 0.76 to 0.80, and the average values of QSLT and baseline mechanisms are 0.79 and 0.78, separately. QSLT is more secure than the baseline mechanism in terms of the 5 K-bits sequence. Besides, in terms of the 25 K-bit sequence, we can achieve that QSLT has a higher average pass ratio (0.78 in Figure 5(c)) compared with the average value of baseline mechanism (0.77 in Figure 5(c)). Therefore, we could conclude that QSLT mechanism is more secure to generate a cryptography key for IoT networks.

5.1.2. Machine Learning Model Tests. This paper also evaluates the security performance of QSLT and the baseline mechanisms by using machine learning models. Particularly, the QRNGs and PRNGs, which are used by QSLT and the baseline mechanisms, affect the performances and behaviors of various machine learning models (e.g., support vector machines) that require a random input [41]. Therefore, this paper selects the classical Support Vector Machines (SVM) classification model [45] to evaluate the randomness of QSLT and baseline mechanisms, i.e., the security performance of quantum keys and classical cryptography keys. The SVM is a supervised machine learning algorithm that learns by example to assign labels to objects, i.e., uses classification algorithms for two-group classification problems. For instance, an SVM algorithm can learn to recognize fraudulent credit card activity by examining hundreds or thousands of fraudulent and nonfraudulent credit card activity reports.

The classification algorithm is a supervised machine learning technique that is used to categorize new observations. In classification, a program makes use of the dataset or observations that are provided to learn how to categorize fresh observations into various classes or groups. For examples, spam or not spam and cat or dog. Typically, The classical SVM classification algorithm includes four steps: 1) reduce data dimensions by applying the principal component analysis if necessary, this is because a model trained with too many dimensions of data is likely to overfit the



(a) The iris dataset

(b) The cancer dataset

(c) The wine dataset

Figure 6: The security results of machine learning model tests.

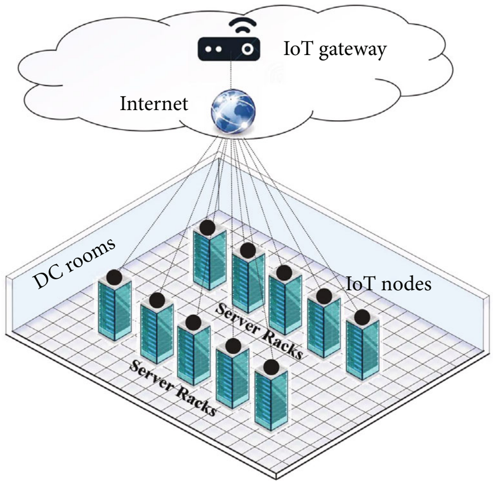


Figure 7: The experimental topology.

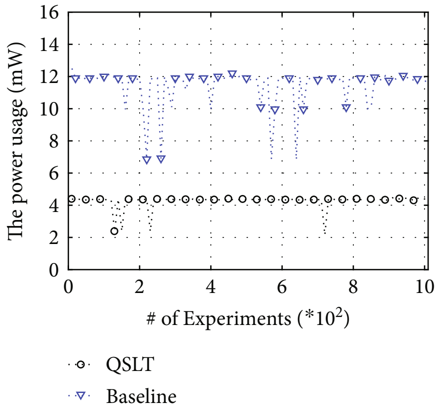


Figure 8: The power usage results.

training dataset and therefore may not perform well on new data. 2) Balance the amount of data and use cross-validation. We separate the data into two groups: one for training and the other for model validation which can be divided in a ratio of 70%/30%. 3) Initialize the weights of the SVM model randomly and train the model using the training dataset. 4) Evaluate the SVM model using the validation data. If the accuracy is less than or equal to 50%, that model will not be useful. If the accuracy reaches 90% or more, that model could be useful.

In our experiments, QSLT and the baseline mechanisms are compared in terms of the iris, breast cancer, and wine datasets [46]. Particularly, the iris dataset has four features (i.e., sepal length, sepal width, petal length, and petal width) and 150 samples total. The breast cancer dataset has 32 features, 569 rows, and a classification for each row of either a malignant cancer tumor or a benign cancer tumor. The wine

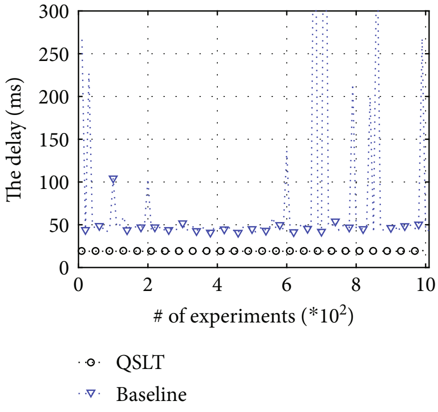


Figure 9: The transmission delay results.

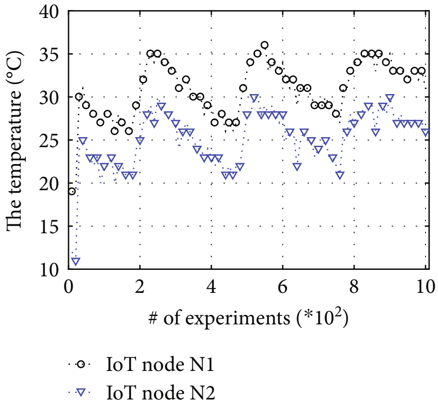


Figure 10: The temperature results.

dataset has 13 features, 178 rows, and a classification of one of three types of wine. It is noting that each dataset is split into the train (70%) and test sets (30%) for the cross-validation. Besides, two different SVMs, i.e., the classical SVM and quantum-based SVM, are implemented by using the Python sklearn [47] and qiskit libraries [48], separately. The sklearn is a module integrating a wide range of state of the art machine learning algorithms for medium-scale supervised and unsupervised problems. The qiskit is an open-source software simulator for quantum computing provided by IBM. Moreover, each experiment is repeated 100 times to eliminate the effect of uncontrollable environmental factors, e.g., temperature and humidity variations. All the source codes can be found via GitHub (The codes can be found via: https://github.com/KB00100100/paper-QSLT). All the experiments are run on a computer that has 6-core 3.59GHz CPU and 24GB RAM resources.

Figure 6 depicts the experimental results. Particularly, the dots marked with 'V' and '*' are raw data of classification accuracies, and the (dash) lines are average accuracy values of different machine learning algorithms. Regarding the iris dataset, the accuracies of all mechanisms are varied from 0.75 to 1. The average accuracy of QSLT is 94.35%, which is larger than the average accuracy of baseline mechanism (94.12% in Figure 6(a)). Regarding the breast cancer dataset, the accuracies of all mechanisms are varied from 0.78 to 1. QSLT also performs better than the baseline mechanism, because the average values of QSLT and baseline mechanisms are 93.88% and 93.14%, separately. Regarding the wine dataset, the accuracies of all mechanisms are varied from 0.75 to 1. QSLT has an average 97.48% accuracy and performs better than the baseline mechanism (97.26% in Figure 6 (c)). Therefore, we could conclude that QSLT has a better randomness. That is, QSLT is more secure than the baseline mechanism.

5.2. The Transmission Performance. To compare the effectiveness of QSLT with QKD-based mechanisms, this paper also evaluates the transmission delay and power usage. Figure 7 depicts the experimental topology. Particularly, there are 10 IoT nodes deployed in our DC rooms, and an IoT gateway deployed in the central cloud. Each node has a 4G module to communicate with the gateway. Besides, the QSLT mechanism is implemented and installed on both IoT gateway and nodes. For comparison, the classical QKD-based mechanism is also simulated as a baseline mechanism [17]. In our experiments, each node collects and uploads temperature data to the gateway every 10 minutes and continues the process for one week. Both QSLT and baseline mechanisms are used to upload the data, and the power usage and transmission delay of all mechanisms are evaluated during the experiments. It is noting that only experimental programs can be run on IoT nodes to make a fair comparison between QSLT and baseline mechanisms. Besides, each experiment is repeated 1,000 times to eliminate the effect of uncontrollable environmental factors, e.g., temperature and humidity variations.

Figures 8–10 show the experimental results. In particular, QSLT and the baseline mechansims cost around 4.35 mW and 10.55 mW power, separately. It is obvious that QSLT decreases the power usage by approximately 58.77% compared with the baseline mechanism. That is, QSLT is more lightweight and has less power usage than the baseline mechanism. Regarding the transmission delay, as shown in Figure 9, the experimental values of QSLT and the baseline mechanisms are around 18.98 ms and 68.65 ms, separately. Besides, this paper also demonstrates the temperature data collected by IoT nodes, and the results are shown in Figure 10. The temperature is fluctuant whose value is from 10°C to 40°C. The average temperature of N1 and N2 nodes are about 30.77°C and 25.19°C, separately.

6. Limitations

This section discusses the limitations of QSLT mechanism in terms of the security, storage, and efficiency performances.

(1) *The Security Limitation*. QSLT has an in-band key-selection field to negotiate session keys between different IoT devices. The key-selection field is important because it indicates which quantum key is used for traffic sessions. However, in this paper, the field is in the form of plaintext and might be a vulnerability for eavesdroppers to launch attacks. Although

eavesdroppers do not know the quantum keys stored locally on IoT devices via SIM cards, they might successfully guess what the quantum key is by using the key-selection field. In the future works, we will consider to encrypt the key-selection field using symmetry/asymmetry cryptographic algorithms

(2) *The Storage Limitation*. To avoid establishing expensive quantum channels among IoT devices, QSLT stores quantum keys locally on IoT devices via SIM cards. The SIM cards have small and fixed memory storage space which leads to a limited number of quantum keys. In terms of our engineering practice, a typical SIM card can store 100,000 quantum keys. In other words, these limited quantum keys can support secure communications for only 100,000 traffic sessions. Any other traffic sessions can only use second-handed and outdated quantum keys. Recycling the quantum keys introduces security vulnerabilities, which might be cracked by eavesdroppers

(3) *The Efficiency Limitation*. Although QSLT mechanism does not need to establish quantum channels compared with traditional QKD-based solutions, it costs a variable-length field in each packet header to indicate which quantum key is used to encrypt/decrypt the packet payload. In other words, QSLT inserts a key-selection field into the headers of traffic packets and costs variable bits of the headers whose lengths depend on the pool size of quantum keys. For example, a typical SIM card can store 100,000 quantum keys based on our engineering experience, i.e., QSLT costs a 14-bit key-selection field to negotiate quantum keys among IoT devices

7. Conclusion

This paper has proposed a novel lightweight transmission mechanism (named QSLT) against eavesdropping attacks for secured data exchanges in IoT networks. QSLT has three steps to ensure secure IoT data transmission: (1) chooses one quantum key to encrypt IoT data; (2) inserts a key-selection field at the end of the encrypted data to ‘tell’ other devices the key’s sequence number; and (3) extracts the key-selection field after receiving the data and decrypts the data with the selected quantum key stored locally on IoT devices. We have implemented the QSLT mechanism and compared its performance with state of the art mechanisms. Experimental results show that the QSLT’s quantum keys have a better security performance for IoT devices against eavesdropping attacks. Besides, QSLT can also transmit IoT data with a lower delay and decreases the power usage by around 58.77% compared with QKD-based mechanisms.

In the future work, we will further integrate the QSLT mechanism with more other IoT narrow-band protocols (e.g., Zigbee). Besides, we will intend to establish quantum communication channels for IoT devices and design a quantum key distribution mechanism against eavesdropping attacks. Moreover, we will also evaluate the effectiveness for QSLT mechanism using high performance hardware devices.

Data Availability

The source data used to support the findings of this study have been deposited in the GitHub repository (https://github.com/KB00100100/paper-QSLT).

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research was funded by the Fundamental Network Research Programs of China Telecom (Grant nos. P-2022-10, T-2022-19, I-2022-07).

References

[1] P. Chamoso, A. González-Briones, S. Rodríguez, and J. M. Corchado, “Tendencies of technologies and platforms in smart cities: a state-of-the-art review,” *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 3086854, 17 pages, 2018.

[2] D. Minoli and B. Occhiogrosso, “Practical aspects for the integration of 5g networks and IoT applications in smart cities environments,” *Wireless Communications and Mobile Computing*, vol. 2019, Article ID 5710834, 30 pages, 2019.

[3] Z. Qin, Z. Cheng, C. Lin, Z. Lu, and L. Wang, “Optimal workload allocation for edge computing network using application prediction,” *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 5520455, 13 pages, 2021.

[4] L. Bai, M. Hu, M. Liu, and J. Wang, “Bpiiot: A light-weighted blockchain-based platform for industrial iot,” *IEEE Access*, vol. 7, pp. 58381–58393, 2019.

[5] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, “A survey on the internet of things (Iot) forensics: challenges, approaches, and open issues,” *IEEE Communication Surveys and Tutorials*, vol. 22, no. 2, pp. 1191–1221, 2020.

[6] J. Gu, J. Wang, Z. Yu, and K. Shen, “Traffic-based side-channel attack in video streaming,” *IEEE/ACM Transactions on Networking*, vol. 27, no. 3, pp. 972–985, 2019.

[7] A. Karati, C.-I. Fan, and R.-H. Hsu, “Provably secure and generalized signcryption with public verifiability for secure data transmission between resource-constrained Iot devices,” *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10431–10440, 2019.

[8] J. Liu, N. Sha, W. Yang, J. Tu, and L. Yang, “Hierarchical q-learning based uav secure communication against multiple uav adaptive eavesdroppers,” *Wireless Communications and Mobile Computing*, vol. 2020, Article ID 8825120, 15 pages, 2020.

[9] J. H. Anajemba, C. Iwendi, M. Razzak, J. A. Ansere, and I. M. Okpalaoguchi, “A counter-eavesdropping technique for optimized privacy of wireless industrial iot communications,” *IEEE Transactions on Industrial Informatics*, vol. 18, no. 9, pp. 6445–6454, 2022.

[10] S.-Y. Tan, K.-W. Yeow, and S. O. Hwang, “Enhancement of a lightweight attribute-based encryption scheme for the internet

of things," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6384–6395, 2019.

[11] K. Muhammad, R. Hamza, J. Ahmad, J. Lloret, H. Wang, and S. W. Baik, "Secure surveillance framework for iot systems using probabilistic image encryption," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3679–3689, 2018.

[12] G. Liu, W. Quan, N. Cheng et al., "Softwarized Iot network immunity against eavesdropping with programmable data planes," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6578–6590, 2021.

[13] K. Sakai, M.-T. Sun, W. S. Ku, J. Wu, and T. H. Lai, "Secure data communications in wireless networks using multi-path avoidance routing," *IEEE Transactions on Wireless Communications*, vol. 18, no. 10, pp. 4753–4767, 2019.

[14] A. A. Abd El-Latif, B. Abd-El-Atty, S. E. Venegas-Andraca et al., "Providing end-to-end security using quantum walks in iot networks," *IEEE Access*, vol. 8, pp. 92687–92696, 2020.

[15] A. A. Abd El-Latif, B. Abd-El-Atty, W. Mazurczyk, C. Fung, and S. E. Venegas-Andraca, "Secure data encryption based on quantum walks for 5g internet of things scenario," *IEEE Transactions on Network and Service Management*, vol. 17, no. 1, pp. 118–131, 2020.

[16] H. Wen, C. Zhang, P. Chen et al., "A quantum chaotic image cryptosystem and its application in Iot secure communication," *IEEE Access*, vol. 9, pp. 20481–20492, 2021.

[17] H. A. Al-Mohammed and E. Yaacoub, "On the use of quantum communications for securing Iot devices in the 6g era," in *2021 IEEE International Conference on Communications Workshops (ICC Workshops)*, pp. 1–6, Montreal, QC, Canada, 2021.

[18] X. Meng, X. Yu, W. Chen, Y. Zhao, and J. Zhang, "Residual-adaptive key provisioning in quantum-key-distribution enhanced internet of things (q-iot)," in *2020 International Wireless Communications and Mobile Computing (IWCMC)*, pp. 2022–2027, Limassol, Cyprus, 2020.

[19] W. Ma, L. Liu, B. Chen, M. Gao, H. Chen, and J. Wu, "Routing, wavelength and time-slot assignment approaches with security level in qkd-enabled optical networks," in *2020 Asia Communications and Photonics Conference (ACP) and International Conference on Information Photonics and Optical Communications (IPOC)*, pp. 1–3, Beijing, China, 2020.

[20] H. Jeon, J. Choi, S. W. McLaughlin, and J. Ha, "Channel aware encryption and decision fusion for wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 4, pp. 619–625, 2013.

[21] R. Tennekoon, J. Wijekoon, and H. Nishi, "On the effectiveness of iproutable entire-packet encryption service over public networks (november 2018)," *IEEE Access*, vol. 6, pp. 73170–73179, 2018.

[22] J. Song, X. Yi, and X. Zhang, *Enhancing Ipsec Performance and Security against Eavesdropping*, US Patent, 2015.

[23] M. Liyanage, A. Braeken, A. D. Jurcut, M. Ylianttila, and A. Gurtov, "Secure communication channel architecture for software defined mobile networks," *Computer Networks*, vol. 114, pp. 32–50, 2017.

[24] L. Wang, H. Kim, P. Mittal, and J. Rexford, "Programmable in-network obfuscation of traffic," https://arxiv.org/abs/2006.00097, 2020.

[25] A. A. Abd El-Latif, B. Abd-El-Atty, I. Mehmood, K. Muhammad, S. E. Venegas-Andraca, and J. Peng, "Quantum-inspired blockchain-based cybersecurity: securing smart edge utilities in IoT-based smart cities," *Information Processing & Management*, vol. 58, no. 4, article 102549, 2021.

[26] S. N. Ghorpade, M. Zennaro, B. S. Chaudhari, R. A. Saeed, H. Alhumyani, and S. Abdel-Khalek, "A novel enhanced quantum pso for optimal network configuration in heterogeneous industrial iot," *IEEE Access*, vol. 9, pp. 134022–134036, 2021.

[27] A. Sharma and A. P. Bhatt, "Quantum cryptography for securing Iot-based healthcare systems," *Limitations and Future Applications of Quantum Cryptography*, pp. 124–147, 2021.

[28] A. A. Abd EL-Latif, B. Abd-El-Atty, E. M. Abou-Nassar, and S. E. Venegas-Andraca, "Controlled alternate quantum walks based privacy preserving healthcare images in internet of things," *Optics & Laser Technology*, vol. 124, article ???, 2020.

[29] A. P. Bhatt and A. Sharma, "Quantum cryptography for internet of things security," *Journal of Electronic Science and Technology*, vol. 17, no. 3, pp. 213–220, 2019.

[30] H. A. Al-Mohammed, A. Al-Ali, E. Yaacoub et al., "Machine learning techniques for detecting attackers during quantum key distribution in Iot networks with application to railway scenarios," *IEEE Access*, vol. 9, pp. 136994–137004, 2021.

[31] H. Ma and B. Chen, "An authentication protocol based on quantum key distribution using decoy-state method for heterogeneous Iot," *Wireless Personal Communications*, vol. 91, no. 3, pp. 1335–1344, 2016.

[32] A. Mavromatis, F. Ntavou, E. H. Salas, G. T. Kanellos, R. Nejabati, and D. Simeonidou, "Experimental demonstration of quantum key distribution (qkd) for energyefficient software-defined internet of things," in *2018 European Conference on Optical Communication (ECOC)*, pp. 1–3, Rome, Italy, 2018.

[33] M. Kaur and S. Kalra, "Security in Iot-based smart grid through quantum key distribution," Advances in computer and computational sciences, 2018.

[34] A. A. Abd El-Latif, B. Abd-El-Atty, M. S. Hossain, S. Elmougy, and A. Ghoneim, "Secure quantum steganography protocol for fog cloud Internet of Things," *IEEE access*, vol. 6, pp. 10332–10340, 2018.

[35] R.-X. Wang, "Quantum secure data transfer with pulse shape encoded optical qubits," *Quantum Engineering*, vol. 3, no. 4, article e81, 2021.

[36] F. Amato, H. M. Torun, and G. D. Durgin, "Beyond the limits of classic backscattering communications: a quantum tunneling rfid tag," in *2017 IEEE International Conference on RFID (RFID)*, pp. 20–25, Phoenix, AZ, USA, 2017.

[37] Y.-G. Yang, H. Lei, Z.-C. Liu, Y.-H. Zhou, and W.-M. Shi, "Arbitrated quantum signature scheme based on cluster states," *Quantum Information Processing*, vol. 15, no. 6, pp. 2487–2497, 2016.

[38] W. Guo, J.-Z. Zhang, Y.-P. Li, and W. An, "Multi-proxy strong blind quantum signature scheme," *International Journal of Theoretical Physics*, vol. 55, no. 8, pp. 3524–3536, 2016.

[39] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, "Quantum random number generation," *npj Quantum Information*, vol. 2, no. 1, pp. 1–9, 2016.

[40] K. Marton and A. Suciu, "On the interpretation of results from the nist statistical test suite," *Science and Technology*, vol. 18, no. 1, pp. 18–32, 2015.

[41] J. J. Bird, A. Ekárt, and D. R. Faria, "On the effects of pseudorandom and quantum-random number generators in soft

computing," *Soft Computing*, vol. 24, no. 12, pp. 9243–9256, 2020.

[42] L. E. Bassham, A. L. Rukhin, J. Soto et al., *Sp 800-22 rev. 1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, National Institute of Standards & Technology, 2010.

[43] G. Aleksandrowicz, T. Alexander, P. Barkoutsos et al., "Qiskit: an open-source framework for quantum computing," *Accessed on*, vol. 16, 2019.

[44] M. Matsumoto and T. Nishimura, "Mersenne twister," *ACM Transactions on Modeling and Computer Simulation (TOMACS)*, vol. 8, no. 1, pp. 3–30, 1998.

[45] L. Wang, "Support vector machines: theory and applications," *Support Vector Machines: Theory and Applications*, vol. 177, 2005.

[46] N. Nguyen and K.-C. Chen, "Quantum embedding search for quantum machine learning," *IEEE Access*, vol. 10, pp. 41444–41456, 2022.

[47] F. Pedregosa, G. Varoquaux, A. Gramfort et al., "Scikit-learn: machine learning in python," *Journal of Machine Learning Research*, vol. 12, pp. 2825–2830, 2011.

[48] A. Cross, "The ibm q experience and qiskit open-source quantum computing software," *APS March meeting abstracts*, vol. 2018, p. L58, 2018.