**Alanezi, AD, El-Latif, AAA, Kolivand, H and Abd-El-Atty, B**

**Quantum walks-based simple authenticated quantum cryptography protocols for secure wireless sensor networks**

**https://researchonline.ljmu.ac.uk/id/eprint/21996/**

**Article**

New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG IOP Institute of Physics

# Quantum walks-based simple authenticated quantum cryptography protocols for secure wireless sensor networks

To cite this article: Ahmad Alanezi *et al* 2023 *New J. Phys.* **25** 123041

New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

OPEN ACCESS

RECEIVED
25 March 2023

REVISED
8 November 2023

ACCEPTED FOR PUBLICATION
1 December 2023

PUBLISHED
22 December 2023

PAPER

# Quantum walks-based simple authenticated quantum cryptography protocols for secure wireless sensor networks

Ahmad Alanezi[1,2], Ahmed A Abd El-Latif[3,4,*], Hoshang Kolivand[1,2] and Bassem Abd-El-Atty[5]

[1] School of Computer Science and Mathematics, Faculty of Engineering and Technology, Liverpool John Moores University (LJMU), Liverpool, L3 3AF, United Kingdom
[2] School of Computing and Digital Technologies, Staffordshire University, United Kingdom
[3] Center of Excellence in Quantum and Intelligent Computing, Prince Sultan University, Riyadh, 11586, Saudi Arabia
[4] Department of Mathematics and Computer Science, Faculty of Science, Menoufia University, Shebin El-Koom, Egypt
[5] Department of Computer Science, Faculty of Computers and Information, Luxor University, Luxor 85957, Egypt
[*] Author to whom any correspondence should be addressed.

**E-mail:** aabdellatif@psu.edu.sa

**Keywords:** authentication, quantum cryptography, quantum key distribution, quantum hash function, quantum walks, wireless sensors, secure communications

## Abstract

Wireless sensor networks (WSNs) play a crucial role in various applications, ranging from environmental monitoring to industrial automation that require high levels of security. With the development of quantum technologies, many security mechanisms may be hacked due to the promising capabilities of quantum computation. To address this challenge, quantum protocols have emerged as a promising solution for enhancing the security of wireless sensor communications. One of the common types of quantum protocols is quantum key distribution (QKD) protocols, which are investigated to allow two participants with fully quantum capabilities to share a random secret key, while semi-quantum key distribution (SQKD) protocols are designed to perform the same task using fewer quantum resources to make quantum communications more realizable and practical. Quantum walk (QW) plays an essential role in quantum computing, which is a universal quantum computational paradigm. In this work, we utilize the advantages of QW to design three authenticated quantum cryptographic protocols to establish secure channels for data transmission between sensor nodes: the first one is authenticated quantum key distribution (AQKD), the second one is authenticated semi-quantum key distribution (ASQKD) with one of the two participants having limited quantum capabilities, and the last one is ASQKD but both legitimate users possess limited quantum resources. The advantages of the proposed protocols are that the partners can exchange several different keys with the same exchanged qubits, and the presented protocols depend on a one-way quantum communication channel. In contrast, all previously designed SQKD protocols rely on two-way quantum communication. Security analyses prove that the presented protocols are secure against various well-known attacks and highly efficient. The utilization of the presented protocols in wireless sensor communications opens up new avenues for secure and trustworthy data transmission, enabling the deployment of resilient WSNs in critical applications. This work also paves the way for future exploration of quantum-based security protocols and their integration into WSNs for enhanced data protection.

## 1. Introduction

Wireless sensor networks (WSNs) have become a ubiquitous technology in modern society, offering versatile communication platforms for various applications. These networks play a crucial role in fields such as monitoring, logistics, surveillance, smart homes, and healthcare [1], where ensuring high levels of security is paramount [2, 3]. However, with the advancements in quantum technologies, many traditional security mechanisms employed in WSNs are at risk of being compromised. The remarkable computational power of quantum computers poses a significant threat to conventional cryptographic algorithms, potentially rendering them vulnerable to attacks [4–6]. As a result, there is a growing need for new cryptographic mechanisms that leverage the principles of quantum computing to enhance the security and privacy of WSNs.

Quantum information and quantum computation are two fields of contemporary scientific research that are now undergoing a lab-to-market transition. The solid results and potential advantages of quantum information and quantum computation have been a powerful attractor for mathematicians, computer scientists, physicists, and engineers, who drive new trends in innovations in information theory, communication, computation, and cryptography.

Quantum key distribution (QKD) is one such quantum-based cryptographic mechanism that holds promise for securing WSNs. QKD allows for the generation and distribution of encryption keys with provable security based on the laws of quantum mechanics [7–9]. It enables the secure exchange of cryptographic keys between sensor nodes, ensuring confidentiality and integrity of the transmitted data. BB84, the first QKD protocol [10], enables two participants to establish a random secret key between each other using quantum states prepared in different bases. In [11], Fan-Yuan *et al* introduced a novel networking scheme for measurement-device-independent QKD. This scheme exhibits robustness against environmental disturbances and offers adaptability for multi-user access. Unlike traditional QKD schemes, this approach enables more than two users to generate keys simultaneously, regardless of the need to align reference frames and compensate for channel disturbances affecting polarization. The authors in [12] proposed a non-standalone measurement-device-independent strategy as an evolutionary selection for existing phase-encoding BB84 networks. Nowadays, in addition to QKD, quantum cryptography includes several other branches of quantum technology, like quantum secret sharing and quantum authentication protocols, among others [13].

In QKD techniques, it is commonly assumed that legitimate participants require full access to quantum resources to securely distribute a random secret key. This includes the capability to prepare and measure qubits in different bases as well as perform unitary operations on qubits. However, there has been research interest in exploring whether it is possible to achieve private key generation with only partial access to quantum resources by utilizing a mixture of classical and quantum resources. This interest has led to the development of protocols known as semi-quantum key distribution (SQKD) or quantum-classical key distribution. SQKD protocols aim to leverage the advantages of both classical and quantum resources to achieve secure key distribution while reducing the overall requirement for quantum capabilities. In [14], Boyer *et al* (BKM07) presented the first SQKD protocol using four quantum states, in which quantum Alice can share with classical Bob a random secret key. Since then, several SQKD protocols have been presented [15–21]. For example, Boyer *et al* [15] presented two SQKD protocols similar to BKM07, the first one is based on randomization and the other is rely on measure-resend. In [16], Zou *et al* showed that the BKM07 protocol can be implemented using less than four quantum states and presented several SQKD protocols using less than four quantum states. Also, Zhang *et al* [17] designed a multi-user SQKD protocol with $m$-classical receiver, and in [18], Wang *et al* presented an SQKD protocol based on quantum entangled states.

If communicating participants do not verify the counterpart's identity, an eavesdropper is able to carry out any active attack, like man-in-the-middle attack and impersonation attack. That is, an eavesdropper Eve imitates Bob (Alice) to communicate with Alice (Bob). Thereby, Eve can get full or at least partial access to the transmitted confidential data of legal participants without being noticed at all. To solve this problem, authentication is a necessary task for data integrity, which is a vital topic in information security. Therefore, authentication plays a crucial role in various quantum cryptography protocols [22], which it serves as a fundamental task to establish trust and ensure the integrity of communications between legitimate parties.

Most quantum cryptographic protocols involve classical channels which play a vital task in eavesdropping detection. The usefulness of such classical channels is closely related to the existence of authentication protocols since, without this feature, quantum protocols would suffer from active attacks performed by undetected eavesdroppers [20, 23, 24]. To construct secure quantum cryptography protocols without authenticated classical channels, various authenticated quantum protocols have been designed [25–30], in which authentication is fulfilled with a pre-shared secret key and discussion over public classical channels. For example, based on Bell states, Zeng and Zhang [25] have designed an authenticated quantum key distribution (AQKD) protocol. Zeng *et al*'s protocol uses a trusted information center in the initial phase. The role of this information center is to help the legitimate participants to establish the secret key. In 2013, based on Bell states, Lin *et al* [26] proposed a multi-user AQKD protocol with star network topology which utilizes a keyed hash function to ensure the identities of participants. In 2014, Yu *et al* [31] designed two authenticated SQKD (ASQKD) protocols using Bell states, which required a pre-shared master key. In [32], Meslouhi *et al* pointed out that the protocol presented in [31] suffered from man-in-the-middle attack. In [29], Yuan *et al* designed a quantum authentication protocol based on ping-pong method. Yuan *et al*'s protocol can verify the identity of legitimate participants and update the initial authentication key for reuse. In [30], Guan *et al* presented a three-party AQKD protocol to share a random secret key between two parties with the help of a trusted center. However, Luo *et al* [33] pointed out that the protocol presented in [30] suffers from information leakage and intercept-measure attack. In 2016, Huang *et al* [27] presented two AQKD protocols based on single photons and the idea of collective detection. The first protocol is a two-party AQKD, and the other protocol is a multiparty AQKD with star network topology. In both protocols, the legitimate participants pre-share an *m-bit* secret key. In [34], Li *et al* presented two ASQKD protocols without classical channels.

Hash functions play a critical role in various cryptographic tasks and are an essential component of modern cryptographic applications [35]. They are widely used in both classical and quantum cryptography to ensure data integrity, authentication, and confidentiality. In the context of quantum authentication protocols, classical hash functions are extensively employed to enhance the security of the established quantum channel [27, 28, 34].

The development of quantum computers and quantum algorithms may endangered some classical cryptographic methods [36]. Simultaneously, several novel proposals using quantum systems to strengthen classical cryptographic protocols have been developed, among them the use of quantum walks (QWs), a universal quantum computation model [37, 38], which can be utilized to create hash functions [36, 39–43] because of its nonlinear chaotic dynamical behavior. Furthermore, QWs have high sensitivity to initial states, non-periodicity, stability and can be used as a tool to produce very large keyspaces capable of withstanding different attacks [44–47].

In quantum cryptographic protocols, privacy amplification is a crucial process that ensures the security of the generated secret key. The purpose of privacy amplification is to remove any potential correlations or knowledge that the eavesdropper may have acquired during the key generation process. The quantum hash function (QHF) that has been constructed using QWs can be used perfectly for privacy amplification [39]. In order to enhance the security of quantum cryptographic protocols, we investigate three authenticated quantum cryptography protocols based on QHF that have been constructed using quantum walks. The first protocol is AQKD and the other two protocols are ASQKD.

Any SQKD protocol relies on a two-way quantum communication (qubits are allowed to travel from the sender to the receiver, then back again to the sender), in which the quantum user (Alice) sends a quantum state to the classical user (Bob) [48]. The classical user is limited to performing the following operations: (1) to measure the received particle in computational basis (Z-basis), (2) to prepare fresh qubits in the computational basis, (3) to reflect qubits, and (4) to reorder qubits.

To reduce the amount of consumed quantum resources to establish a random secret key between two parties, Krawec [49] and Liu and Hwang [50] presented a SQKD protocol to establish a random secret key in which two classical participants utilize a mediated server with quantum capabilities. In all above-mentioned SQKD and ASQKD protocols, users are actually semi-classical users as they require some quantum resources for preparing qubits in computational basis or quantum memory to reorder qubits [20]. In this paper, we present two ASQKD protocols that reduce the consumed quantum resources for establishing a random secret key with participants sensor nodes. In the first protocol, the receiver node (Bob) has access to those quantum resources only necessary for running QWs and measuring qubits in the computational basis. In the second protocol, both legitimate participants nodes are semi-classical. The sender node (Alice) has access only to those quantum resources required to run QWs, as well as to prepare and send qubits in the computational basis $\{|0\rangle,|1\rangle\}$, while the receiver node has access to the quantum resources needed to measure qubits in the computational basis as well as to run QWs. For distinguishing between the proposed two ASQKD protocols, we call the first as ASQKD1 (has one semi-classical user) and the other as ASQKD2 (both users are semi-classical). We can summarize the role of QWs in designing the proposed protocols as follows: (1) act as a QHF for the privacy amplification technique with higher security; (2) decide the encoding basis for the transmitted qubits; (3) decide the measurement basis for the received qubits and its positions; and (4) perform the authentication process between legitimate parties for the proposed protocols.

Some key properties of our proposed quantum cryptography protocols are:

(i) The pre-shared control parameters are numerical values and can be reused several times due to both the pre-shared key and some publicly announced parameters being used as control parameters for the QW.

(ii) The authenticated members can establish different secret keys with the same established qubits because the privacy amplification process is based on both the output of established qubits and some publicly announced parameters. By announcing different parameters, the legitimate parties obtain different shared keys without any potential correlations between them.

(iii) The number of bits for the shared secret key may be greater than the number of shared qubits several times due to performing the privacy amplification process.

(iv) In order to reduce the cost of the consumed quantum resources in practical implementations, the proposed ASQKD protocols rely on one-way quantum communication channel while the previous presented ASQKD and SQKD protocols based on two-way quantum communication.

The layout of this paper is set as follows: the presented scenario for wireless sensors communications in quantum scenario is provided in section 2, while the preliminary knowledge for QWs is given in sections 3 and 4 is devoted to the proposed authenticated quantum cryptography protocols. The analysis of the suggested protocols is given in section 5 and the conclusion drowns in section 6.

## 2. WSNs scenario

WSNs have become a fundamental technological component for intelligent communities because of their potential benefits. The applications of WSNs extend from body area networks to local and home area networks and further to a wide variety of services in smart cities [51]. However, applications of WSNs lack stringent privacy and security protection due to the involvement of human life.

The architecture of WSNs and the restricted nature of the node's resources make it vulnerable and open to numerous attacks. In addition, an adversary can intercept and hereafter fabricate sensitive data to be transmitted as the original data. Moreover, an attacker can pass incorrect data and even reveal it as a sensor itself, and modify the collected data. If the communication of sensor nodes is not secure, then a malicious entity can extract the transmitted data and the code associated with that node, which leads to many security threats and challenges.

Also, with the development of quantum technologies, many cryptographic mechanisms may be hacked due to the promising capabilities of quantum computers. Therefore, security and privacy are the foremost challenges for WSNs, which need new cryptographic mechanisms to have the ability to withstand the promising attacks from digital computers besides quantum computers. For these reasons, the goal of this paper is to design new authentication protocols for secure wireless communication based on quantum technologies and open the door for integrating quantum technologies with WSNs and various Internet of Things devices to achieve high security and efficiency. The suggested scenario for wireless sensor communications in the quantum scenario is presented in figure 1.

## 3. QWs based QHF

A coined discrete QW is composed of the following elements: a walker, a coin, evolution operators for both coin and walker and a set of observables. A walker is a quantum system $|\psi\rangle_p$ exists in a Hilbert space $\mathcal{H}_p$ of dimension $d$ where $d = N$ for a QW run on an $N$-node circle. The coin is typically a quantum system existing in a two-dimensional Hilbert space $|\psi\rangle_c \in \mathcal{H}_c$. In each step $t$ of acting QWs, a Unitary operator $\hat{U}$ applied on the entire quantum state $|\varphi\rangle$

$$\hat{U} = \hat{S}\left(\hat{I} \otimes \hat{C}\right) \tag{1}$$

where $\hat{C}$ is a Unitary operator to be applied on the coin state, $\hat{I}$ is the identity operator, and $\hat{S}$ is the Shift operator (that is, the operator that diffuses the quantum particle over the topology over which the QW is run). If the QW is run over an $N$ circle, then the shift operator $\hat{S}$ can be expressed as in equation (2)

$$\begin{aligned}\hat{S} = &\textstyle\sum_{x\notin\{1,N\}} |x+1,0\rangle\langle x,0| + |x-1,1\rangle\langle x,1| \\ &+ \textstyle\sum_{x\in\{1\}} |2,0\rangle\langle 1,0| + |N,1\rangle\langle 1,1| \\ &+ \textstyle\sum_{x\in\{N\}} |1,0\rangle\langle N,0| + |N-1,1\rangle\langle N,1|.\end{aligned} \tag{2}$$

The coin operator $\hat{C}$ can be written in matrix for as in equation (3)

$$\begin{pmatrix} \cos\ \theta & \sin\ \theta \\ \sin\ \theta & -\cos\ \theta \end{pmatrix}, where\ \ \theta \in [0, \pi]. \tag{3}$$

The final state $|\varphi\rangle_{\text{final}}$ of the quantum state after $t$ steps is provided by equation (4)

$$|\varphi\rangle_{\text{final}} = \left(\hat{U}\right)^t |\varphi\rangle_0. \tag{4}$$

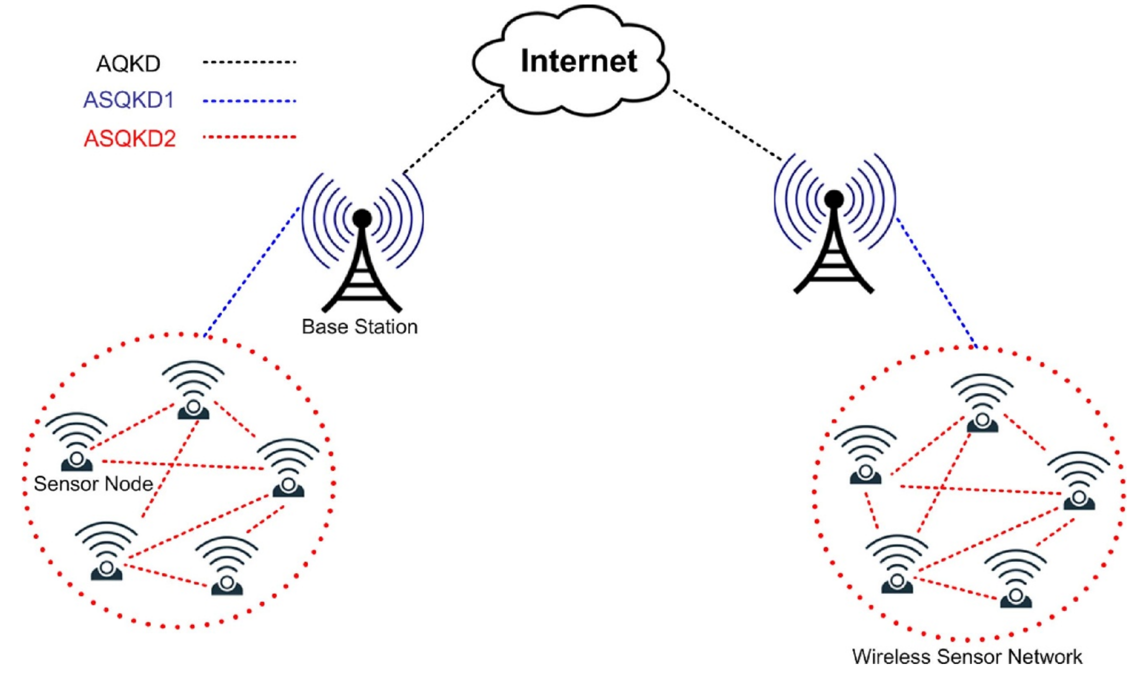


**Figure 1.** The suggested scenario for wireless sensor communications in quantum scenario.

The probability $P(x,t)$ of locating the walker at location $x$ after $t$ steps can be represented as in equation (5)

$$P(x,t) = \sum_{i=0}^{1} \left| \langle x,i| \left(\hat{U}\right)^{t} |\psi\rangle_0 \right|^2 . \tag{5}$$

In 2013, Li *et al* [36] proposed the first QHF based on 1-D two-walker QWs on a circle controlled by a bit string. After that, numerous QHFs based on QWs have been constructed [39, 41, 42]. Furthermore, please note that the probability $P(x,t)$ have *nonzero* in any location $x$ if the number of steps $t$ is greater than or equal to the number of vertices $N$ [43, 52]. All constructed QHFs based on QWs [43] survive from this defect. To avoid this defect we will modify the QHF presented in [42] by appending another coin operator.

In [42], Yang *et al* built a QHF for a binary *m-bit* based on one-walker QWs on a circle with $N$ nodes. Unitary operators $\hat{U}_0$ and $\hat{U}_1$ are applied when the $t$th bit of $m$ is *'0'* and *'1'*, respectively. In the modified QHF, we use three coins $\hat{C}_0$, $\hat{C}_1$ and $\hat{C}_2$ to construct the three evolution operators $\hat{U}_0$, $\hat{U}_1$ and $\hat{U}_2$, respectively. Where the evolution operator $\hat{U}_0$ ($\hat{U}_1$) is performed when the $t$th bit of $m$ is *'0'* (*'1'*), and the evolution operator $\hat{U}_2$ is applied when the $t$th step exceeds to the size of $m$ and does not reach $N$. As an example, if $m$ is *'101'* and $N = 25$, the final state can be given as in equation (6)

$$|\varphi\rangle_{\text{final}} = \left(\prod_{t=4}^{25} \hat{U}_2^t\right) \hat{U}_1 \hat{U}_0 \hat{U}_1 |\varphi\rangle_0 . \tag{6}$$

According to QHF presented in [42], the final state can be written as in equation (7)

$$|\varphi\rangle_{\text{final}} = \hat{U}_1 \hat{U}_0 \hat{U}_1 |\varphi\rangle_0 \tag{7}$$

where probability $P$ is equal to *zero* in some locations. For more illustration, the hash values constructed by the two QHFs (modified QHF and Yang *et al*'s QHF [42]) using the same parameters for message $m =$ *'101'* and $N = 25$ are given in figure 2 for binary format and in the hexadecimal format as follows:

- Modified QHF: *9581 D3E3 0E6A 2956 2FB6 E3F7 5298 7609 8C31 A6E3 3B8F B2F4 53*
- Yang *et al*'s QHF [42]: *0000 0000 0000 0000 003F 003F 003F 003F 0000 0000 0000 0000 00*

The modified QHF is outlined in the following steps.

(i) Select initial parameters $(N, m, \omega, \theta_0, \theta_1, \theta_2)$ for operating one-particle QWs on a circle of $N$ vertices governed by *m-bit* to generate a probability distribution $P$ of size $N$. Here $\theta_0$, $\theta_1$ and $\theta_2$ are parameters

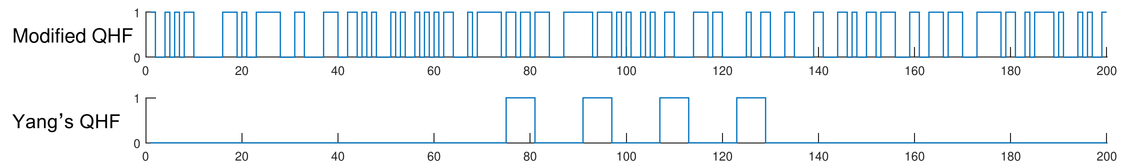


**Figure 2.** Plots of 200-bit hash value constructed by the two QHFs (modified QHF and Yang *et al*'s QHF [42]) using the same parameters for message *'101'* and $N$ is *25*.

for the coin operators $\hat{C}_0$, $\hat{C}_1$ and $\hat{C}_2$, respectively. The coin initial state is prepared as $|\psi\rangle_c = \cos(\omega)|0\rangle + \sin(\omega)|1\rangle$.

(ii) Construct the hash value for $m$ string by transforming $P$ to a binary values as in equation (8):

$$hash = dec2bin\left(fix\left(P_i \times 10^{12}\right)\ mod\ 2^8, 8\right) \tag{8}$$

where $8 \times N$ is the length of binary hash value.

## 4. The proposed quantum authentication protocols

There are two types of participants in any quantum cryptography protocol: quantum participants and semi-quantum (classical) participants. The quantum participant has full quantum capabilities and can prepare, measure, and manipulate complex quantum states using advanced quantum techniques. The classical participant has access to limited quantum resources to carry out the following procedures: (1) receive and resend quantum states via the quantum channel; (2) perform measurements using the computational basis; (3) prepare quantum states on the computational basis; (4) reflect quantum states; and (5) reorder quantum states (that need quantum memory) [20].

This section presents three variants of quantum authentication protocols designed to establish random secret keys based on quantum walks. The first protocol is AQKD and the others are ASQKD, which the proposed protocols required pre-share master key parameters $(\omega, \theta_0, \theta_1, \theta_2)$ for operating one-particle QWs on a circle with odd $N$ nodes (for instance, this can be prepared in advance once in a closed environment). The pre-shared master key parameters are used to establish a common secret key between two or more entities. This process typically involves securely exchanging the pre-shared key parameters through a trusted channel, or it can be prepared in advance in a closed environment. Once the entities have the same pre-shared master key parameters, they can be used as a basis for authentication operations and further cryptographic operations.

In the proposed quantum authentication protocols, the used quantum communication environment is based on single photons, and the quantum channel is assumed to be lossless and noiseless.

### 4.1. The AQKD protocol

The procedure of AQKD protocol is illustrated in figure 3 and given in the following steps:

(i) The sender (Alice) informs the receiver (Bob) publicly an odd number $N$, for performing QHF $(N, \omega, \theta_2)$ to produce a hash value $B \in \{0,1\}^{8N}$ of length $8 \times N$.

(ii) Alice prepares a stream of single photons $S \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}^{8N}$ according to $B$ sequence as follows and records its corresponding classical values $R \in \{0,1\}^{8N}$. $B$ decides the encoding bases. If the $i$th bit of $B$ is *'1'* then Alice randomly prepares the qubit $S_i$ in computational basis (Z-basis) as $|0\rangle$ or $|1\rangle$. Moreover, if the $i$th bit of $B$ is *'0'* then Alice randomly prepares the qubit $S_i$ in Hadamard basis (X-basis) as $|+\rangle$ or $|-\rangle$.

(iii) Alice transmits the photon stream $S$ to Bob through an ideal quantum channel.

(iv) As Bob receives the photon sequence $S$, he measures the qubits with correct bases according to the bit string $B$. If the $i$th bit of $B$ is *'1'* then Bob measures the qubit $S_i$ in the computational basis. Furthermore, if the $i$th bit of $B$ is *'0'* then Bob measures qubit $S_i$ in Hadamard basis. Thereby, Bob obtains the measurement results $R \in \{0,1\}^{8N}$.

(v) Alice publicly agrees with Bob an odd number $N_{\text{check}}$, to perform QHF $(N_{\text{check}}, R, \omega, \theta_0, \theta_1, \theta_2)$ for creating a bit string $K_{\text{check}} \in \{0,1\}^{8N_{\text{check}}}$ with length $8 \times N_{\text{check}}$.

(vi) For detecting an eavesdropper, Alice informs Bob the first $4 \times N_{\text{check}}$-*bit* of $K_{\text{check}}$ sequence. If the comparing outcomes are identical, then Bob declares the remaining bits of $K_{\text{check}}$ to be reviewed by Alice. Thereby, both partners authenticate each other. If there is any mistake, both members end the protocol.

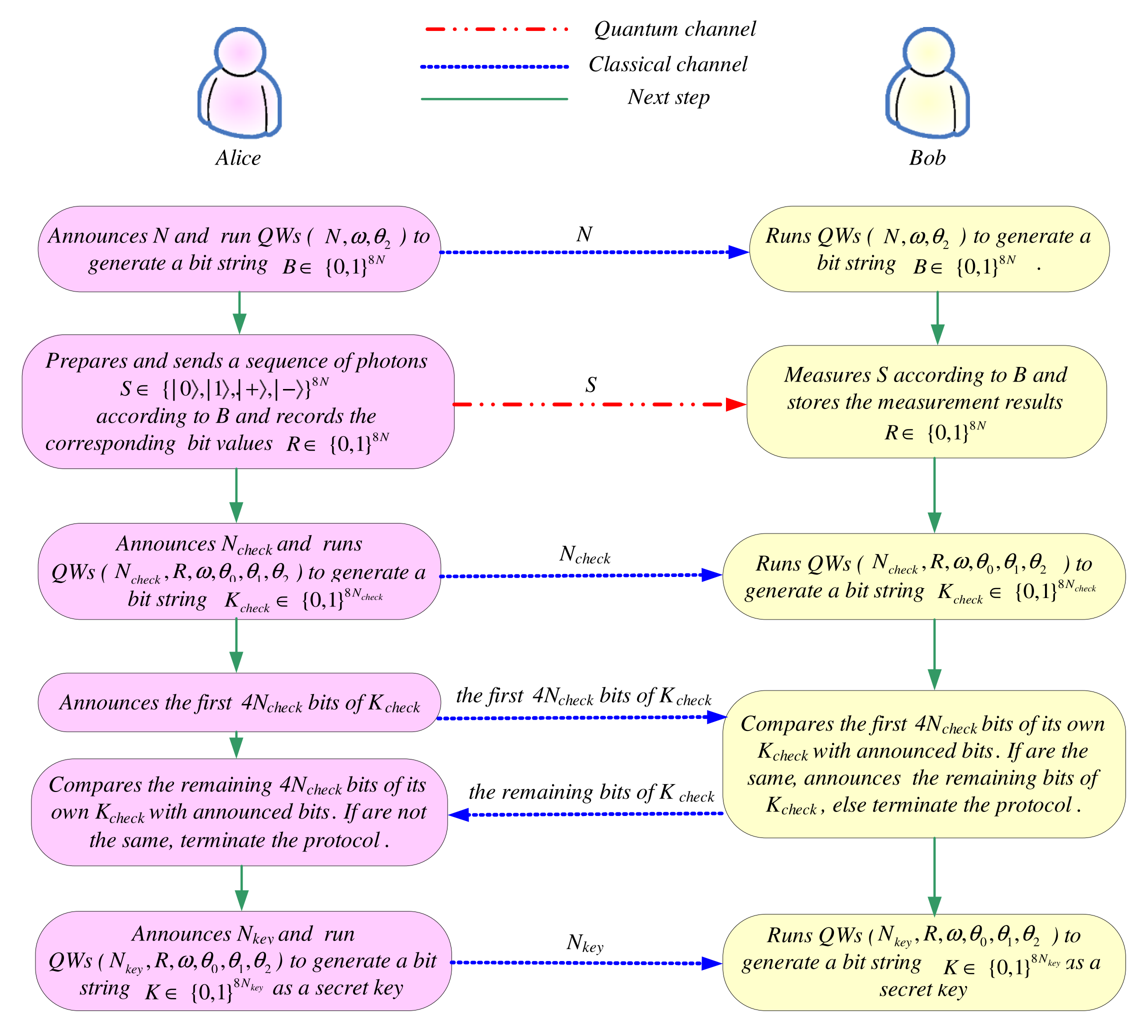

Quantum channel
Classical channel
Next step
Alice
Bob
Announces N and run QWs ( N, ω, θ2 ) to generate a bit string B ∈ {0,1}^8N
N
Runs QWs ( N, ω, θ2 ) to generate a bit string B ∈ {0,1}^8N .
Prepares and sends a sequence of photons S ∈ {|0⟩,|1⟩,|+⟩,|−⟩}^8N according to B and records the corresponding bit values R ∈ {0,1}^8N
S
Measures S according to B and stores the measurement results R ∈ {0,1}^8N
Announces N_check and runs QWs ( N_check, R, ω, θ0, θ1, θ2 ) to generate a bit string K_check ∈ {0,1}^8N_check
N_check
Runs QWs ( N_check, R, ω, θ0, θ1, θ2 ) to generate a bit string K_check ∈ {0,1}^8N_check
Announces the first 4N_check bits of K_check
the first 4N_check bits of K_check
Compares the first 4N_check bits of its own K_check with announced bits. If are the same, announces the remaining bits of K_check, else terminate the protocol.
Compares the remaining 4N_check bits of its own K_check with announced bits. If are not the same, terminate the protocol.
the remaining bits of K_check
Announces N_key and run QWs ( N_key, R, ω, θ0, θ1, θ2 ) to generate a bit string K ∈ {0,1}^8N_key as a secret key
N_key
Runs QWs ( N_key, R, ω, θ0, θ1, θ2 ) to generate a bit string K ∈ {0,1}^8N_key as a secret key

**Figure 3.** The proposed AQKD protocol, which both the legitimate users have fully quantum capabilities and the size of the exchanged final key is dependent on the stated $N_{\mathrm{key}}$ only and not on the number of shared qubits.

(vii) Eventually, Alice informs Bob an odd number $N_{\mathrm{key}}$, to operates QWs $(N_{\mathrm{key}}, R, \omega, \theta_0, \theta_1, \theta_2)$ for constructing the hash value $K \in \{0,1\}^{8N_{\mathrm{key}}}$ as a secret key of length $8\times N_{\mathrm{key}}$ bits.

From the declared data via the classical channel around the hash value, no one can get any information regarding the master key $(\omega, \theta_0, \theta_1, \theta_2)$ or the final secret key $K$. Consequently, the master key can be reused several times later due to both the pre-shared key and some publicly announced parameters being used as control parameters for operating QW and performing the privacy amplification process. Also, there are no potential correlations between the shared final keys and the measurement results $R$ or any information regarding the master key. For more illustration, see the given example in figure 4, in which both authorized partners can establish various secret keys utilizing the same transmitted qubits by replicating step (vii) various times with publishing another $N_{\mathrm{key}}$ in each time.

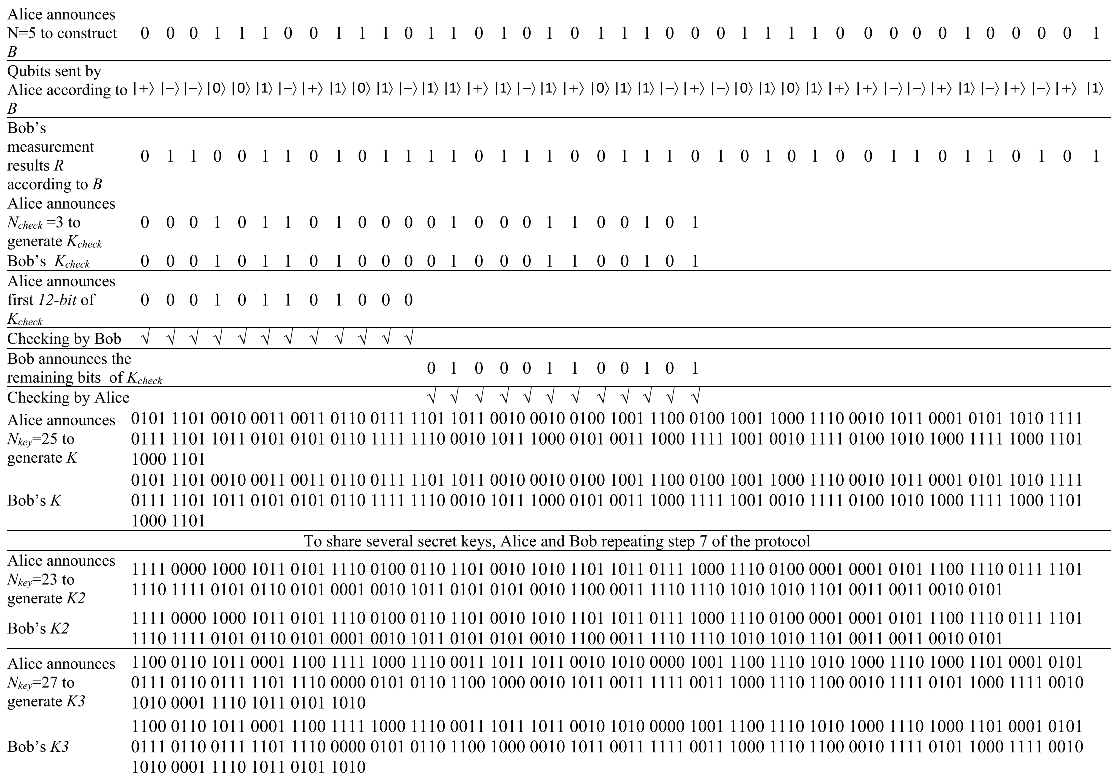
### 4.2. The ASQKD1 protocol

In any SQKD protocol, Alice with fully quantum capabilities communicates with the classical receiver (Bob) to establish a random secret key via two-way quantum communication channel. The main contribution of presenting this class of protocols is to reduce the quantum capabilities to make quantum communications more realizable and practical. Therefore, the proposed ASQKD1 protocol relies on one-way quantum communication and Bob has limited quantum capabilities to execute the following operations: (1) receives and measures qubits with computational basis, and (2) runs one-walker quantum walks on a circle.

The procedures of ASQKD1 protocol are given in figure 5 and described in the following steps:

(i) Perform step (i) as in our AQKD protocol (section 4.1).

(ii) Alice prepares a stream of single photons $S \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}^{8N}$ according to $B$ sequence as follows: Let $B$ decides the encoding bases. If the $i$th bit of $B$ is '*1*', then Alice randomly prepares the qubit



| | |
|---|---|
| Alice announces N=5 to construct *B* | 0 0 0 1 1 1 0 0 1 1 1 0 1 1 0 1 0 1 0 1 1 1 0 0 0 1 1 1 1 0 0 0 0 0 1 0 0 0 0 1 |
| Qubits sent by Alice according to *B* | $|+\rangle$ $|-\rangle$ $|-\rangle$ $|0\rangle$ $|0\rangle$ $|1\rangle$ $|-\rangle$ $|+\rangle$ $|1\rangle$ $|0\rangle$ $|1\rangle$ $|-\rangle$ $|1\rangle$ $|1\rangle$ $|+\rangle$ $|1\rangle$ $|-\rangle$ $|1\rangle$ $|+\rangle$ $|0\rangle$ $|1\rangle$ $|1\rangle$ $|-\rangle$ $|+\rangle$ $|-\rangle$ $|0\rangle$ $|1\rangle$ $|0\rangle$ $|1\rangle$ $|+\rangle$ $|+\rangle$ $|-\rangle$ $|-\rangle$ $|+\rangle$ $|1\rangle$ $|-\rangle$ $|+\rangle$ $|-\rangle$ $|+\rangle$ $|1\rangle$ |
| Bob's measurement results *R* according to *B* | 0 1 1 0 0 1 1 0 1 0 1 1 1 1 0 1 1 1 0 0 1 1 1 0 1 0 1 0 1 0 0 1 1 0 1 1 0 1 0 1 |
| Alice announces $N_{check}$ =3 to generate $K_{check}$ | 0 0 0 1 0 1 1 0 1 0 0 0 0 1 0 0 0 1 1 0 0 1 0 1 |
| Bob's $K_{check}$ | 0 0 0 1 0 1 1 0 1 0 0 0 0 1 0 0 0 1 1 0 0 1 0 1 |
| Alice announces first *12-bit* of $K_{check}$ | 0 0 0 1 0 1 1 0 1 0 0 0 |
| Checking by Bob | √ √ √ √ √ √ √ √ √ √ √ √ |
| Bob announces the remaining bits of $K_{check}$ | 0 1 0 0 0 1 1 0 0 1 0 1 |
| Checking by Alice | √ √ √ √ √ √ √ √ √ √ √ √ |
| Alice announces $N_{key}$=25 to generate *K* | 0101 1101 0010 0011 0011 0110 0111 1101 1011 0010 0010 0100 1001 1100 0100 1001 1000 1110 0010 1011 0001 0101 1010 1111 0111 1101 1011 0101 0101 0110 1111 1110 0010 1011 1000 0101 0011 1000 1111 1001 0010 1111 0100 1010 1000 1111 1000 1101 1000 1101 |
| Bob's *K* | 0101 1101 0010 0011 0011 0110 0111 1101 1011 0010 0010 0100 1001 1100 0100 1001 1000 1110 0010 1011 0001 0101 1010 1111 0111 1101 1011 0101 0101 0110 1111 1110 0010 1011 1000 0101 0011 1000 1111 1001 0010 1111 0100 1010 1000 1111 1000 1101 1000 1101 |
| To share several secret keys, Alice and Bob repeating step 7 of the protocol | |
| Alice announces $N_{key}$=23 to generate *K2* | 1111 0000 1000 1011 0101 1110 0100 0110 1101 0010 1010 1101 1011 0111 1000 1110 0100 0001 0001 0101 1100 1110 0111 1101 1110 1111 0101 0110 0101 0001 0010 1011 0101 0101 0010 1100 0011 1110 1110 1010 1010 1101 0011 0011 0010 0101 |
| Bob's *K2* | 1111 0000 1000 1011 0101 1110 0100 0110 1101 0010 1010 1101 1011 0111 1000 1110 0100 0001 0001 0101 1100 1110 0111 1101 1110 1111 0101 0110 0101 0001 0010 1011 0101 0101 0010 1100 0011 1110 1110 1010 1010 1101 0011 0011 0010 0101 |
| Alice announces $N_{key}$=27 to generate *K3* | 1100 0110 1011 0001 1100 1111 1000 1110 0011 1011 1011 0010 1010 0000 1001 1100 1110 1010 1000 1110 1000 1101 0001 0101 0111 0110 0111 1101 1110 0000 0101 0110 1100 1000 0010 1011 0011 1111 0011 1000 1110 1100 0010 1111 0101 1000 1111 0010 1010 0001 1110 1011 0101 1010 |
| Bob's *K3* | 1100 0110 1011 0001 1100 1111 1000 1110 0011 1011 1011 0010 1010 0000 1001 1100 1110 1010 1000 1110 1000 1101 0001 0101 0111 0110 0111 1101 1110 0000 0101 0110 1100 1000 0010 1011 0011 1111 0011 1000 1110 1100 0010 1111 0101 1000 1111 0010 1010 0001 1110 1011 0101 1010 |

**Figure 4.** An illustrated paradigm for the presented AQKD protocol, in the case of the pre-established master key is $\omega = 0, \theta_0 = 60, \theta_1 = 45$, and $\theta_2 = 36$.

$S_i$ in computational basis as $|0\rangle$ or $|1\rangle$, and records the corresponding classical bit value of *i*th qubit as $R \in \{0,1\}^x$. Otherwise, Alice randomly prepares the qubit $S_i$ with diagonal basis as $|+\rangle$ or $|-\rangle$.

(iii) Perform step (iii) as in our AQKD protocol (section 4.1).

(iv) As Bob receives a photon stream *S*, he performs quantum measurements in computational basis on each incoming qubit and stores the corresponding measurement results of *i*th qubit when *i*th bit of *B* is *'1'* to get the classical bit string $R \in \{0,1\}^x$.

(v) Performing steps (v)–(vii) in the proposed AQKD protocol, which presented in section 4.1.

Figure 6 illustrates our ASQKD1 protocol.

### 4.3. The ASQKD2 protocol

In our ASQKD2 protocol, both legitimate participants have access to both classical and quantum resources: Alice has access only to those quantum resources required to send and prepare qubits in the computational basis, and running quantum walks, while Bob has access to those quantum resources needed to receive and measure qubits with the computational basis as well as for running quantum walks. Our ASQKD2 protocol relies on one-way quantum communication, not rely on two-way quantum communication as stated in the previous presented SQKD protocols.

The procedure of ASQKD2 protocol is illustrated in figure 7 and presented as follows:

(i) Perform step (i) as in our AQKD protocol (section 4.1)

(ii) Alice produces a random sequence of single photons $S \in \{|0\rangle, |1\rangle\}^{8N}$ using the computational basis and records the corresponding classical values of *i*th qubit when *i*th bit of *B* is *'1'*.

(iii) Performing step (iii) in the proposed AQKD protocol.

(iv) As Bob receives a photon stream *S*, he measures all received qubits using the computational basis and stores the measurement results of *i*th qubit when *i*th bit of *B* is *'1'*, to get the classical bit string $R \in \{0,1\}^x$.

(v) Perform steps (v)–(vii) in the proposed AQKD protocol, as presented in section 4.1.

The main contribution of proposing ASQKD2 is to share a random secret key between two semi-quantum participants without using a mediated quantum server, to reduce the amount of consumed

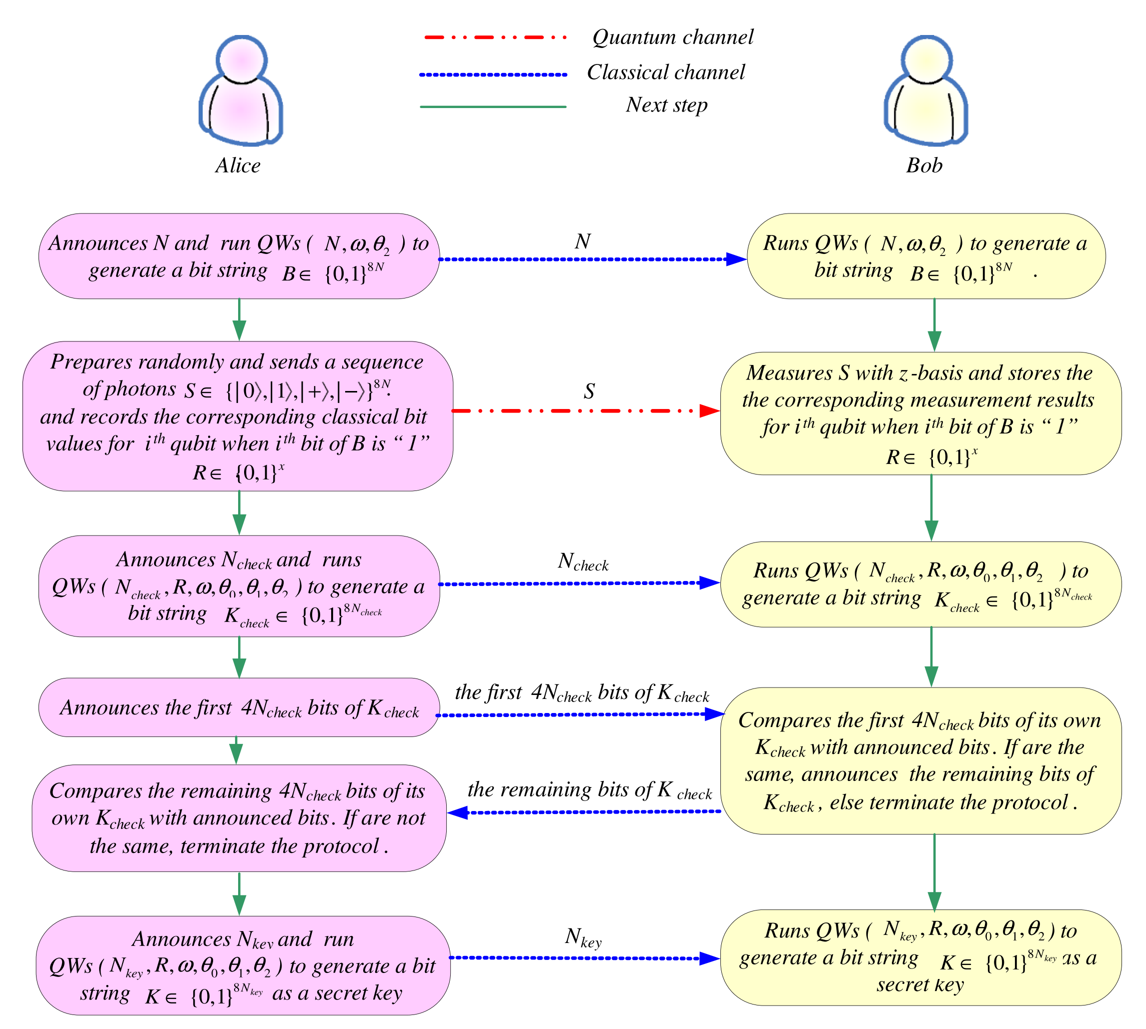

Quantum channel
Classical channel
Next step
Alice
Bob
Announces N and run QWs ( $N, \omega, \theta_2$ ) to generate a bit string $B \in \{0,1\}^{8N}$
N
Runs QWs ( $N, \omega, \theta_2$ ) to generate a bit string $B \in \{0,1\}^{8N}$ .
Prepares randomly and sends a sequence of photons $S \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}^{8N}$. and records the corresponding classical bit values for $i^{th}$ qubit when $i^{th}$ bit of B is " 1" $R \in \{0,1\}^{x}$
S
Measures S with z-basis and stores the the corresponding measurement results for $i^{th}$ qubit when $i^{th}$ bit of B is " 1" $R \in \{0,1\}^{x}$
Announces $N_{check}$ and runs QWs ( $N_{check}, R, \omega, \theta_0, \theta_1, \theta_,$ ) to generate a bit string $K_{check} \in \{0,1\}^{8N_{check}}$
$N_{check}$
Runs QWs ( $N_{check}, R, \omega, \theta_0, \theta_1, \theta_2$ ) to generate a bit string $K_{check} \in \{0,1\}^{8N_{check}}$
Announces the first $4N_{check}$ bits of $K_{check}$
the first $4N_{check}$ bits of $K_{check}$
Compares the first $4N_{check}$ bits of its own $K_{check}$ with announced bits. If are the same, announces the remaining bits of $K_{check}$, else terminate the protocol .
Compares the remaining $4N_{check}$ bits of its own $K_{check}$ with announced bits. If are not the same, terminate the protocol .
the remaining bits of $K_{check}$
Announces $N_{key}$ and run QWs ( $N_{key}, R, \omega, \theta_0, \theta_1, \theta_2$ ) to generate a bit string $K \in \{0,1\}^{8N_{key}}$ as a secret key
$N_{key}$
Runs QWs ( $N_{key}, R, \omega, \theta_0, \theta_1, \theta_2$ ) to generate a bit string $K \in \{0,1\}^{8N_{key}}$ as a secret key

**Figure 5.** The proposed ASQKD1 protocol, which Alice has fully quantum capabilities and Bob limited to measures qubits with computational basis, besides of running quantum walks.

quantum resources and to make quantum communications more realizable and practical. For more illustration see the example presented in figure 8.

## 5. Analysis of the presented protocols

In this section, we prove that the proposed authenticated quantum cryptography protocols are high efficient and secure against several well-known attacks such as intercept-and-resend attack, impersonation attack, and collective attack.

### 5.1. Efficiency analysis

One of the essential tools to measure the efficiency of quantum protocols is the qubit efficiency, which presented by Cabello [53] and can be denoted as follows:

$$\eta_{\text{qubit}} = \frac{K}{B + C} \tag{9}$$

where $K$ is the total number of bits for the established secret key, $B$ represents the number of whole generated qubits, and $C$ refers to the number of whole exchanged classical bits over the classical channel except those used for eavesdropping check [54]. One of the main advantages of QHF based on quantum walks is the length of the hash value variant with the number of nodes in the circle. In the proposed protocols, Alice informs Bob of a value for $N$, to run QWs $(N, \omega, \theta_2)$ to produce a hash value $B \in \{0,1\}^{8N}$ with length $8 \times N$ (step (i)), and announces another odd integer number $N_{\text{key}}$, to run QWs $(N_{\text{key}}, R, \omega, \theta_0, \theta_1, \theta_2)$ to generate a hash value $K \in \{0,1\}^{8N_{\text{key}}}$ with length $8 \times N_{\text{key}}$ as a secret key (step (vii)). Therefore, the qubit efficiency of the proposed authenticated quantum cryptography protocols is dependent only on the number of nodes in

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Alice announces $N=5$ to construct $B$ | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 |
| Qubits sent by Alice according to $B$ | $\|-\rangle$ | $\|+\rangle$ | $\|-\rangle$ | $\|1\rangle$ | $\|0\rangle$ | $\|1\rangle$ | $\|-\rangle$ | $\|+\rangle$ | $\|1\rangle$ | $\|0\rangle$ | $\|0\rangle$ | $\|-\rangle$ | $\|1\rangle$ | $\|1\rangle$ | $\|+\rangle$ | $\|1\rangle$ | $\|-\rangle$ | $\|1\rangle$ | $\|+\rangle$ | $\|0\rangle$ | $\|1\rangle$ | $\|0\rangle$ | $\|+\rangle$ | $\|-\rangle$ | $\|+\rangle$ | $\|0\rangle$ | $\|1\rangle$ | $\|1\rangle$ | $\|0\rangle$ | $\|-\rangle$ | $\|+\rangle$ | $\|-\rangle$ | $\|+\rangle$ | $\|+\rangle$ | $\|1\rangle$ | $\|+\rangle$ | $\|+\rangle$ | $\|-\rangle$ | $\|+\rangle$ | $\|0\rangle$ |
| Recorded $R$ by Alice | | | | 1 | 0 | 1 | | | 1 | 0 | 0 | | 1 | 1 | | 1 | | 1 | | 0 | 1 | 0 | | | | 0 | 1 | 1 | 0 | | | | | | 1 | | | | | 0 |
| Bob's measurement results $R$ according to $B$ | | | | 1 | 0 | 1 | | | 1 | 0 | 0 | | 1 | 1 | | 1 | | 1 | | 0 | 1 | 0 | | | | 0 | 1 | 1 | 0 | | | | | | 1 | | | | | 0 |
| Alice announces $N_{check}=3$ to generate $K_{check}$ | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | | | | | | | | | | | | | | | | |
| Bob's $K_{check}$ | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | | | | | | | | | | | | | | | | |
| Alice announces first *12-bit* of $K_{check}$ | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Checking by Bob | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Bob announces the remaining bits of $K_{check}$ | | | | | | | | | | | | | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | | | | | | | | | | | | | | | | |
| Checking by Alice | | | | | | | | | | | | | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | | | | | | | | | | | | | | | | |
| Alice announces $N_{key}=25$ to generate $K$ | 1110 1010 0101 0111 1110 0011 1010 0111 0000 0111 0010 1101 1001 1000 1000 0111 0100 1111 0100 0110 1011 1000 0101 0111 0100 0101 0001 0011 0111 1000 0011 1110 1111 1001 0000 1000 1111 0011 1110 0111 1001 0000 1011 0010 0100 1011 1111 1010 1011 1110 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Bob's $K$ | 1110 1010 0101 0111 1110 0011 1010 0111 0000 0111 0010 1101 1001 1000 1000 0111 0100 1111 0100 0110 1011 1000 0101 0111 0100 0101 0001 0011 0111 1000 0011 1110 1111 1001 0000 1000 1111 0011 1110 0111 1001 0000 1011 0010 0100 1011 1111 1010 1011 1110 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| To share several secret keys, Alice and Bob repeating step 7 of the protocol | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Alice announces $N_{key}=23$ to generate $K2$ | 0100 0101 1110 1011 0111 0111 1100 1110 1000 0110 0111 0001 0110 1001 1010 0001 0001 0111 1100 0010 1001 0000 1101 0101 0111 0101 1011 1100 0110 0000 0000 1010 0000 1111 0111 1001 1000 1001 0011 1110 0000 0110 0001 1100 0011 0001 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Bob's $K2$ | 0100 0101 1110 1011 0111 0111 1100 1110 1000 0110 0111 0001 0110 1001 1010 0001 0001 0111 1100 0010 1001 0000 1101 0101 0111 0101 1011 1100 0110 0000 0000 1010 0000 1111 0111 1001 1000 1001 0011 1110 0000 0110 0001 1100 0011 0001 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Figure 6.** An illustrated paradigm for the presented ASQKD1 protocol, in the case of the pre-established master key is $\omega = 0, \theta_0 = 60, \theta_1 = 45$, and $\theta_2 = 36$.

the circle $(N, N_{\text{key}})$ announced by Alice for running quantum walks. If the number $N_{\text{key}}$ announced by Alice is greater than $N$ several times, then the number of bits for the shared secret key $K$ greater than the number of shared qubits $B$ several times. In the illustrated examples (see figures 4, 6 and 8), Alice announces with Bob via the classical channel 5 (3-bit) for $N$ and 25 (5-bit) for $N_{\text{key}}$, so the total number of classical bits exchanged over the classical channel is 8-bit, the number of whole bits for the shared secret key $K$ is 200-bit, and the total number of generated qubits is 40 qubit. Therefore, the qubit efficiency for the illustrated examples only is $\frac{K}{B+C} = \frac{200}{40+8} = \frac{200}{48} = 4\frac{1}{6}$. Furthermore, the partners can establish various numbers of keys $K$s with the same transferred qubits $B$, by repeating step (vii) several times with announcing different $N_{\text{key}}$ at each time (see figures 4, 6 and 8).

There are also other measures for efficiency, pre-shared key efficiency, which can be stated as in equation (10)

$$\eta_{\text{pre-shared}} = \frac{K}{M} \tag{10}$$

where $K$ is the total number of bits for the established secret key, $M$ represents the total number of bits for the pre-shared master key. The participants of the presented protocols require a pre-share master key parameters $(\omega, \theta_0, \theta_1, \theta_2)$ for acting one-walker quantum walks on a circle with odd $N$ vertices, which are numerical values that typically have a compact representation, requiring less storage space and reducing transmission overhead. This efficiency is particularly beneficial when dealing with large master keys or when transmitting them over limited-bandwidth networks. In the illustrated examples (see figures 4, 6 and 8), $\omega = 0$ (1-bit), $\theta_0 = 60$ (6-bit), $\theta_1 = 45$ (6-bit), and $\theta_2 = 36$ (6-bit). So, the total number of bits for the pre-shared master key is 19-bit. Therefore, the pre-shared key efficiency for the illustrated examples only is $\frac{K}{M} = \frac{200}{19} = 10.53$. Table 1 demonstrates the efficiency of the presented protocols, which gives the qubit efficiency and the pre-shared key efficiency for the proposed authenticated quantum cryptography protocols and its related ASQKD protocols [31, 34]. Subsequently, the proposed protocols are highly efficient.

### 5.2. Security analysis

The main goal of Eve is to get any information about the established key from the transferred qubits. Hence, security analysis is an essential task for any quantum protocol. The security of our proposed quantum cryptography protocols is guaranteed by both standard protocols like the quantum no-cloning theorem and

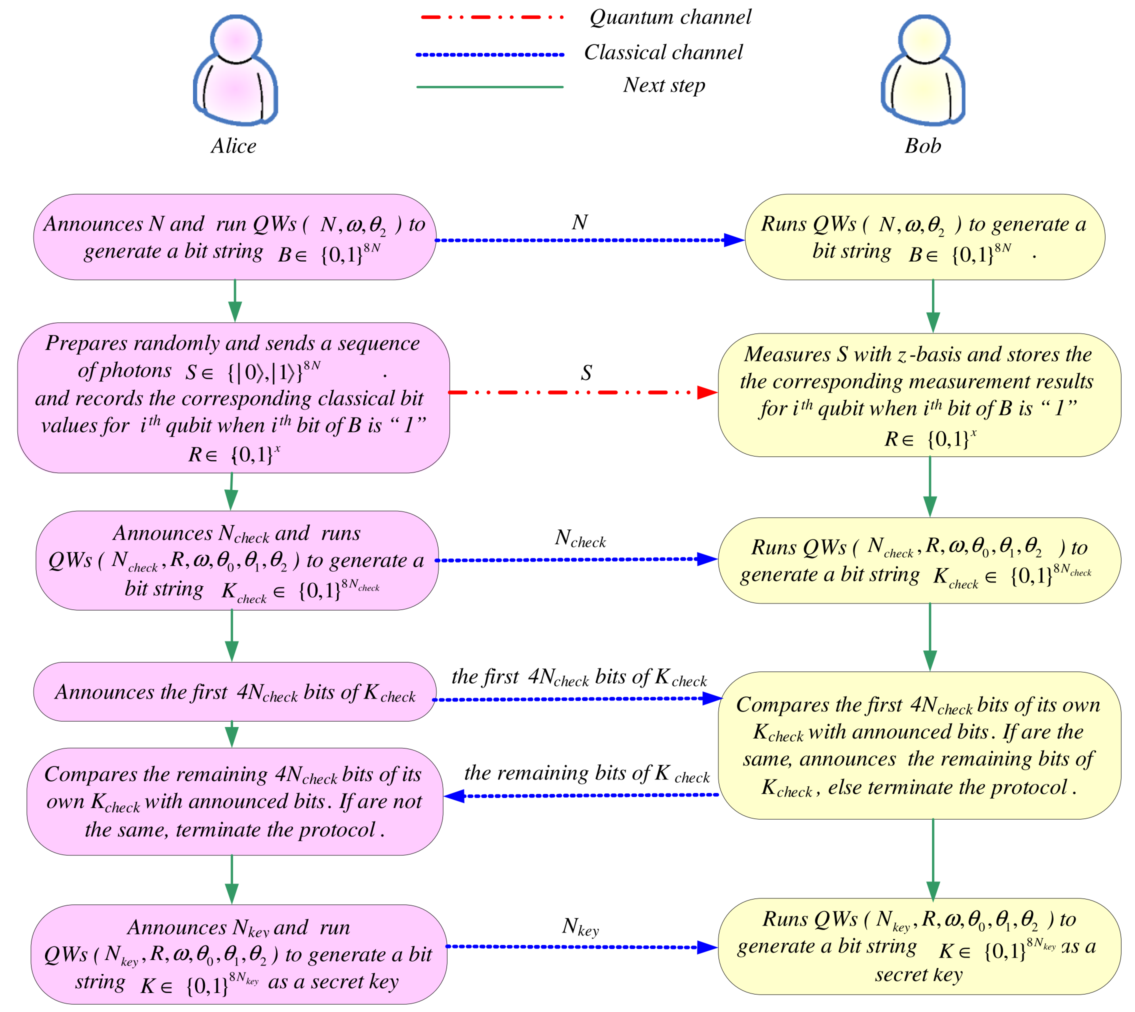

Quantum channel
Classical channel
Next step
Alice
Bob
Announces N and run QWs ( $N, \omega, \theta_2$ ) to generate a bit string $B \in \{0,1\}^{8N}$
N
Runs QWs ( $N, \omega, \theta_2$ ) to generate a bit string $B \in \{0,1\}^{8N}$ .
Prepares randomly and sends a sequence of photons $S \in \{|0\rangle, |1\rangle\}^{8N}$ . and records the corresponding classical bit values for $i^{th}$ qubit when $i^{th}$ bit of B is "1" $R \in \{0,1\}^{x}$
S
Measures S with z-basis and stores the the corresponding measurement results for $i^{th}$ qubit when $i^{th}$ bit of B is "1" $R \in \{0,1\}^{x}$
Announces $N_{check}$ and runs QWs ( $N_{check}, R, \omega, \theta_0, \theta_1, \theta_2$ ) to generate a bit string $K_{check} \in \{0,1\}^{8N_{check}}$
$N_{check}$
Runs QWs ( $N_{check}, R, \omega, \theta_0, \theta_1, \theta_2$ ) to generate a bit string $K_{check} \in \{0,1\}^{8N_{check}}$
Announces the first $4N_{check}$ bits of $K_{check}$
the first $4N_{check}$ bits of $K_{check}$
Compares the first $4N_{check}$ bits of its own $K_{check}$ with announced bits. If are the same, announces the remaining bits of $K_{check}$, else terminate the protocol.
the remaining bits of $K_{check}$
Compares the remaining $4N_{check}$ bits of its own $K_{check}$ with announced bits. If are not the same, terminate the protocol.
Announces $N_{key}$ and run QWs ( $N_{key}, R, \omega, \theta_0, \theta_1, \theta_2$ ) to generate a bit string $K \in \{0,1\}^{8N_{key}}$ as a secret key
$N_{key}$
Runs QWs ( $N_{key}, R, \omega, \theta_0, \theta_1, \theta_2$ ) to generate a bit string $K \in \{0,1\}^{8N_{key}}$ as a secret key

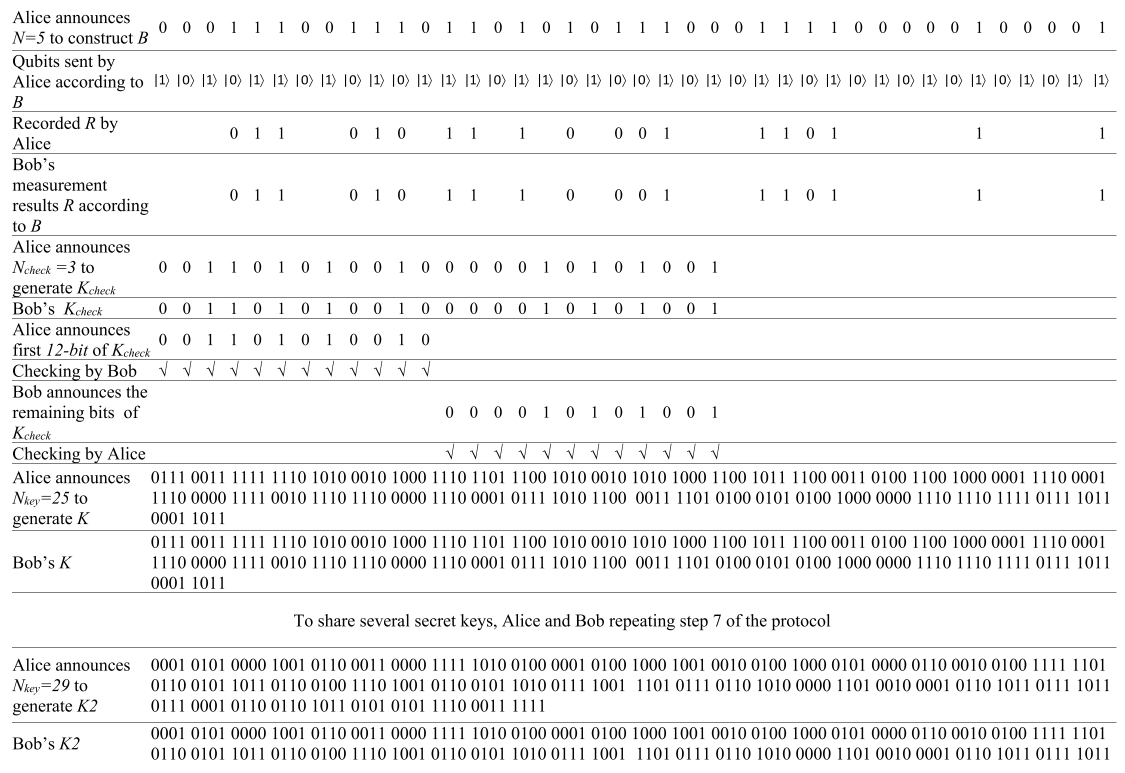
**Figure 7.** The proposed ASQKD2 protocol, which Alice limited to prepare qubits in computational basis and running quantum walks, while Bob limited to measure the received qubits with computational basis besides running quantum walks.

quantum uncertainty postulate to prevent unconditional attacks as well as on quantum walks and their key parameters. In the case of both participants are restricted to quantum capabilities, the key established between them cannot achieve conditional security but its security is based on mathematical computation [21]. However, the security of the two proposed ASQKD protocols is based on quantum walks, not mathematical computation. In this regard, we exhibit the security analysis for the presented protocols in a detailed way and confirm that the presented protocols are effective in exposing any active attack.

### 5.2.1. Impersonation analysis

In these types of attack, Eve plays Bob's role in communicating with Alice, and in other words, plays Alice's role in communicating with Bob to obtain the fully established secret key or part of it.

***In the presented AQKD protocol***, we assumed that Eve impersonates the Alice task to contact Bob. In step (i), Eve announces with Bob the value of $N$, to produce a bit string $B^{'} \in \{0,1\}^{8N}$ by running QWs $(N, \omega, \theta_2)$. Nevertheless, it is extremely difficult to produce the correct hash value $B$, because Eve does not have the full key parameters $(\omega, \theta_2)$. Furthermore, it is very difficult for Eve to prepare a sequence of single photons $S \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}^{8N}$ with correct bases according to $B$. Eventually Eve transfers to Bob a fake stream of photons $S$ according to its own bit string $B^{'}$. In step (iv), Bob measures the received qubits according to the hash value $B$. Then Eve informs Bob about a value for $N_{\text{check}}$, for producing a bit string $K_{\text{check}} \in \{0,1\}^{8N_{\text{check}}}$ by running QWs $(N_{\text{check}}, R, \omega, \theta_0, \theta_1, \theta_2)$. The bit values of $R$ recorded by Eve (step (ii)) is distinct from the measurement results $R$ stored by Bob (step (iv)) due to the generated $B$ stream for both partners is distinct from each other and Eve do not possessing the correct key $\omega, \theta_0, \theta_1$, and $\theta_2$ (step (i)). Therefore, Bob reveals the presence of Eve in step (vi), once Eve publishes the first $4 \times N_{\text{check}}$-bit of $K_{\text{check}}$, thus the protocol terminated by Bob. On the other hand, if Eve wants to play the role of Bob to contact Alice. Eve revealed by



| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Alice announces *N=5* to construct *B* | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 |
| Qubits sent by Alice according to *B* | $\|1\rangle$ | $\|0\rangle$ | $\|1\rangle$ | $\|0\rangle$ | $\|1\rangle$ | $\|1\rangle$ | $\|0\rangle$ | $\|1\rangle$ | $\|0\rangle$ | $\|1\rangle$ | $\|0\rangle$ | $\|1\rangle$ | $\|1\rangle$ | $\|1\rangle$ | $\|0\rangle$ | $\|1\rangle$ | $\|1\rangle$ | $\|0\rangle$ | $\|1\rangle$ | $\|0\rangle$ | $\|0\rangle$ | $\|1\rangle$ | $\|0\rangle$ | $\|1\rangle$ | $\|0\rangle$ | $\|1\rangle$ | $\|1\rangle$ | $\|0\rangle$ | $\|1\rangle$ | $\|0\rangle$ | $\|1\rangle$ | $\|0\rangle$ | $\|1\rangle$ | $\|0\rangle$ | $\|1\rangle$ | $\|0\rangle$ | $\|1\rangle$ | $\|0\rangle$ | $\|1\rangle$ | $\|1\rangle$ |
| Recorded *R* by Alice | | | | 0 | 1 | 1 | | | 0 | 1 | 0 | | 1 | 1 | | 1 | | 0 | | 0 | 0 | 1 | | | | 1 | 1 | 0 | 1 | | | | | | 1 | | | | | 1 |
| Bob's measurement results *R* according to *B* | | | | 0 | 1 | 1 | | | 0 | 1 | 0 | | 1 | 1 | | 1 | | 0 | | 0 | 0 | 1 | | | | 1 | 1 | 0 | 1 | | | | | | 1 | | | | | 1 |
| Alice announces $N_{check}$ *=3* to generate $K_{check}$ | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | | | | | | | | | | | | | | | | |
| Bob's $K_{check}$ | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | | | | | | | | | | | | | | | | |
| Alice announces first *12-bit* of $K_{check}$ | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Checking by Bob | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Bob announces the remaining bits of $K_{check}$ | | | | | | | | | | | | | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | | | | | | | | | | | | | | | | |
| Checking by Alice | | | | | | | | | | | | | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | | | | | | | | | | | | | | | | |
| Alice announces $N_{key}$*=25* to generate *K* | 0111 0011 1111 1110 1010 0010 1000 1110 1101 1100 1010 0010 1010 1000 1100 1011 1100 0011 0100 1100 1000 0001 1110 0001 1110 0000 1111 0010 1110 1110 0000 1110 0001 0111 1010 1100 0011 1101 0100 0101 0100 1000 0000 1110 1110 1111 0111 1011 0001 1011 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Bob's *K* | 0111 0011 1111 1110 1010 0010 1000 1110 1101 1100 1010 0010 1010 1000 1100 1011 1100 0011 0100 1100 1000 0001 1110 0001 1110 0000 1111 0010 1110 1110 0000 1110 0001 0111 1010 1100 0011 1101 0100 0101 0100 1000 0000 1110 1110 1111 0111 1011 0001 1011 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| To share several secret keys, Alice and Bob repeating step 7 of the protocol | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Alice announces $N_{key}$*=29* to generate *K2* | 0001 0101 0000 1001 0110 0011 0000 1111 1010 0100 0001 0100 1000 1001 0010 0100 1000 0101 0000 0110 0010 0100 1111 1101 0110 0101 1011 0110 0100 1110 1001 0110 0101 1010 0111 1001 1101 0111 0110 1010 0000 1101 0010 0001 0110 1011 0111 1011 0111 0001 0110 0110 1011 0101 0101 1110 0011 1111 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Bob's *K2* | 0001 0101 0000 1001 0110 0011 0000 1111 1010 0100 0001 0100 1000 1001 0010 0100 1000 0101 0000 0110 0010 0100 1111 1101 0110 0101 1011 0110 0100 1110 1001 0110 0101 1010 0111 1001 1101 0111 0110 1010 0000 1101 0010 0001 0110 1011 0111 1011 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Figure 8.** An illustrated paradigm for the presented ASQKD2 protocol, in the case of the pre-established master key is $\omega = 0, \theta_0 = 60, \theta_1 = 45$, and $\theta_2 = 36$.

**Table 1.** Qubit efficiency and pre-shared key efficiency for the proposed authenticated cryptography protocols and its related ASQKD protocols [31, 34].

| Protocol | The sender | The receiver | Quantum channel | Quantum information carrier | Pre-shared key efficiency | Qubit efficiency |
|---|---|---|---|---|---|---|
| Proposed AQKD | Fully quantum | Fully quantum | One-way | Single particles | Numerical values for the key parameters and its efficiency is 1053% according to the illustrated examples | Depending on the announced $N$ and $N_{\text{key}}$, and it is 416.67% according to the illustrated examples |
| Proposed ASQKD1 | Fully quantum | Restricted quantum capabilities | | | | |
| Proposed ASQKD2 | Restricted quantum capabilities | Restricted quantum capabilities | | | | |
| Yu *et al*'s [31] ASQKD Randomization -based | Fully quantum | Restricted quantum capabilities | Two-way | Entangled particles | 10% | 12.5% |
| Yu *et al*'s [31] ASQKD Measure -based | | | | Entangled particles | 10% | 10% |
| Li *et al*'s [34] ASQKD Randomization -based | | | | Single particles | 50% | 25% |
| Li *et al*'s [34] ASQKD Measure-based | | | | Entangled particles | 25% | 11.11% |

Alice in step (vi), when Alice informs Eve with the first $4\times N_{\text{check}}$-bit of $K_{\text{check}}$ sequence and waits Eve to response with the remaining bits of $K_{\text{check}}$. By checking the remaining bits announced of $K_{\text{check}}$ , Alice reveals the presence of Eve and terminates the protocol.

As for the security of the proposed ASQKD1 and ASQKD2 protocols, the same analyses can be performed and detect the existence of Eve in step (vi) of each protocol. Therefore, the proposed authenticated quantum cryptography protocols are secure against active attacks. Moreover, Eve does not obtain any information about the master key $(\omega, \theta_0, \theta_1, \theta_2)$ therefore, the key parameters can be used later several times.

### *5.2.2. Intercept-resend analysis*

In this type of attack, Eve tries to obtain any secret information by intercepting the sequence of photons $S$ sent by Alice, and then resends it to Bob.

***In the proposed AQKD protocol***, Eve tries to measure the photons in the sequence $S$ transferred by Alice. Eve does not possess any information regarding the keys $(\omega, \theta_2)$ to measure the transferred qubits in correct bases according to the correct hash value $B$. Ultimately, Eve performs quantum measurement in random bases and then sends it to Bob with a new sequence of photons according to her used measurement bases and corresponding measurement results. Then, Bob measures the received qubits according to the hash value $B$ to obtain a measurement results $R$ (step (iv)) that different from the classical bit values $R$ recorded by Alice (step (ii)). That leads to Bob generate a checking hash value $K_{\text{check}}$ by running QWs $(N_{\text{check}}, R, \omega, \theta_0, \theta_1, \theta_2)$ different from Alice's $K_{\text{check}}$ (step (v)) due to the bit string $R$ is different for both participants. Consequently, both participants detect the presence of Eve and terminate the protocol (step (vi)). Therefore, the proposed AQKD protocol is secure against intercept-resend attack.

***In the proposed ASQKD1 protocol***, Bob performs quantum measurement in computational basis on all received qubits. Eve knows this fact and the protocol is one-way communication, therefore she measures all qubits in computational basis over the sequence $S$ sent by Alice, then prepares a new sequence of photons in computational basis according to her measurement results and sends it to Bob. In step (iv) of the protocol, Bob performs quantum measurement with computational basis on all qubits and stores only the measurement results of $i$th qubit when $i$th bit of $B$ is *'1'* to get the classical bit string $R$. Eve does not have any information regarding to the key parameters $(\omega, \theta_2)$ to store the measurement results when $i$th bit of $B$ is *'1'*, so Eve randomly extract a fake bit string $R^{'}$. In step (vi) of the protocol, Alice and Bob check $K_{\text{check}}$ that there is no detection for the existence of Eve (the quantum channel assumed to be ideal) due to Eve sending to Bob a sequence of photons with computational basis according to her measurement results, so the protocol continues for sharing the random secret key (step (vii)). Eve may be successful to obtain $R$ partly, however, Eve fails to obtain any information regarding the established secret key due to Eve not possessing the used master key parameters for generating the secret key QWs $(N_{\text{key}}, R, \omega, \theta_0, \theta_1, \theta_2)$. Therefore, the proposed ASQKD1 protocol is secure against intercept-resend attack.

Regarding the analysis of the proposed ASQKD2 protocol, the same analysis of the proposed ASQKD1 protocol can be performed.

### *5.2.3. Collective attack*

Collective attacks are a type of security threat that can compromise the integrity of the quantum communication channel. Unlike individual attacks in which Eve interacts with each signal coming from Alice (Bob) separately, in collective attacks, Eve attaches ancilla state to each state transmitted independently between the legitimate parties, Alice and Bob. Eve uses unitary operators to extract the information from the target states to the ancilla states. She then retains her quantum state and retransmits the quantum state originally transmitted between Alice and Bob. Once Alice and Bob complete their state measurements and announce the measurement bases, Eve can store the ancilla states, wait for the participants of the protocol to publish some useful information, and then measure the ancilla states to obtain the information. This method allows Eve to gather information without introducing detectable disturbances and poses a significant threat to the security of the quantum communication system.

***In the proposed AQKD protocol***, Eve attaches the ancilla state to each transmitted photon in the sequence $S$ to Bob. Once Alice and Bob complete their state measurements and announce the hash value $K_{\text{check}}$ to authenticate each other, Eve can measure the ancilla states, trying to obtain some information about the measurement results $R$. But the announced hash value $K_{\text{check}}$ does not help Eve measure the ancilla states on the correct basis, due to the announced hash value $K_{\text{check}}$ being the hash code for the measurement results $R$. Hence, it is hard for Eve to get the correct measurement results $R$. Therefore, the proposed AQKD protocol is secure against collective attack.

***In the proposed ASQKD1 protocol***, Bob performs quantum measurement on computational basis on all received qubits. Eve knows this fact, and the protocol is one-way communication; therefore, she measures all ancilla states on computational basis. Eve does not have any information regarding the key parameters $(\omega, \theta_2)$

to store the measurement results when $i$th bit of $B$ is *'1'*, so Eve may be successful in obtaining $R$ partly. However, Eve fails to obtain any information regarding the established secret key due to Eve not possessing the used master key parameters for generating the secret key QWs $(N_{\text{key}}, R, \omega, \theta_0, \theta_1, \theta_2)$, and tiny changes in the sequence $R$ lead to a massive change in the established secret key. Therefore, the proposed ASQKD1 protocol is secure against collective attack.

Regarding the analysis of the proposed ASQKD2 protocol, the same analysis of the proposed ASQKD1 protocol can be performed.

## 6. Conclusions

In this paper, we used the benefits of quantum walks characteristics to propose three authenticated quantum cryptography protocols based on quantum walks for secure wireless sensor communications: the first one is AQKD, the second is ASQKD with one of the two participants having limited quantum capabilities, and the last protocol is ASQKD with both legitimate users having limited quantum capabilities. The advantages of the proposed quantum cryptography protocols are: (a) the preshared master key parameters can be reused several times; (b) the authenticated partners can establish various secret keys with the same transferred qubits; (c) the number of bits for the shared secret key may be greater than the number of shared qubits several times according to the used $N$ and $N_{\text{key}}$; and (d) the protocols rely on a one-way quantum communication channel, while all previous proposed SQKD protocols rely on two-way quantum communication. Security analyses showed that the proposed protocols are highly efficient and secure against several well-known attacks, such as intercept-and-resend attack, impersonation attack, and collective attack. The main goal of the presented work is to open the door for integrating quantum technologies with WSNs and various Internet of Things devices to achieve high security and efficiency.

## Data availability statement

All data that support the findings of this study are included within the article (and any supplementary files). Data will be available from 25 April 2023.

## Acknowledgments

Ahmed A Abd El-Latif would like to thank the Center of Excellence in Quantum and Intelligent Computing at Prince Sultan University, Saudi Arabia, for the support. Also, the authors warmly thank their families for their unconditional support.

## Author contributions statement

The authors contributed equally to this work.

## References

[1] Anitha S, Jayanthi P and Chandrasekaran V 2021 An intelligent based healthcare security monitoring schemes for detection of node replication attack in wireless sensor networks *Measurement* **167** 108272

[2] Ahmad I, Rahman T, Zeb A, Khan I, Ullah I, Hamam H and Cheikhrouhou O 2021 Analysis of security attacks and taxonomy in underwater wireless sensor networks *Wirel. Commun. Mob. Comput.* **2021** 1–15

[3] Alturki R, Alyamani H J, Ikram M A, Rahman M A, Alshehri M D, Khan F and Haleem M 2021 Sensor-cloud architecture: a taxonomy of security issues in cloud-assisted sensor networks *IEEE Access* **9** 89344–59

[4] Abd-El-Atty B 2022 A robust medical image steganography approach based on particle swarm optimization algorithm and quantum walks *Neural Comput. Appl.* **35** 773–85

[5] Abd-El-Atty B 2022 Quaternion with quantum walks for designing a novel color image cryptosystem *J. Inf. Secur. Appl.* **71** 103367

[6] Abd-El-Atty B, ElAffendi M and El-Latif A A A 2022 A novel image cryptosystem using gray code, quantum walks and henon map for cloud applications *Complex Intell. Syst.* **9** 609–24

[7] Zhou L, Lin J, Jing Y and Yuan Z 2023 Twin-field quantum key distribution without optical frequency dissemination *Nat. Commun.* **14** 928

[8] Wang P, Zhang Y, Lu Z, Wang X and Li Y 2023 Discrete-modulation continuous-variable quantum key distribution with a high key rate *New J. Phys.* **25** 023019

[9] Endo H, Sasaki T, Takeoka M, Fujiwara M, Koashi M and Sasaki M 2022 Line-of-sight quantum key distribution with differential phase shift keying *New J. Phys.* **24** 025008

[10] Bennett C and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing* pp 175–9

[11] Fan-Yuan G-J *et al* 2022 Robust and adaptable quantum key distribution network without trusted nodes *Optica* **9** 812–23

[12] Fan-Yuan G-J, Lu F-Y, Wang S, Yin Z-Q, He D-Y, Zhou Z, Teng J, Chen W, Guo G-C and Han Z-F 2021 Measurement-device-independent quantum key distribution for nonstandalone networks *Photon. Res.* **9** 1881–91

[13] Abd-El-Atty B, Venegas-Andraca S E and El-Latif A A A 2018 Quantum information protocols for cryptography *Quantum Computing: An Environment for Intelligent Large Scale Real Application* (Springer) pp 3–23

[14] Boyer M, Kenigsberg D and Mor T 2007 Quantum key distribution with classical Bob *Phys. Rev. Lett.* **99** 140501

[15] Boyer M, Gelles R, Kenigsberg D and Mor T 2009 Semiquantum key distribution *Phys. Rev.* A **79** 032341

[16] Zou X, Qiu D, Li L, Wu L and Li L 2009 Semiquantum-key distribution using less than four quantum states *Phys. Rev.* A **79** 052312

[17] Zhang X, Gong W and Tan Y 2009 Quantum key distribution series network protocolwith m-classical Bobs *Chin. Phys.* B **18** 2143

[18] Wang J, Zhang S, Zhang Q and Tang C 2011 Semiquantum key distribution using entangled states *Chin. Phys. Lett.* **28** 100301

[19] Krawec W 2016 Security of a semi-quantum protocol where reflections contribute to the secret key *Quantum Inf. Process.* **15** 2067–90

[20] Li Q, Chan W H and Zhang S 2016 Semiquantum key distribution with secure delegated quantum computation *Sci. Rep.* **6** 19898

[21] Zhu K-N, Zhou N-R, Wang Y-Q and Wen X-J 2018 Semi-quantum key distribution protocols with GHZ states *Int. J. Theor. Phys.* **57** 3621–31

[22] Arul R, Raja G, Bashir A K, Chaudry J and Ali A 2018 A console grid leveraged authentication and key agreement mechanism for LTE/SAE *IEEE Trans. Ind. Inf.* **14** 2677–89

[23] Yang C W, Hwang T and Lin T H 2013 Modification attack on QSDC with authentication and the improvement *Int. J. Theor. Phys.* **52** 2230–4

[24] Lin J, Yang C W, Tsai C W and Hwang T 2013 Intercept-resend attacks on semi-quantum secret sharing and the improvements *Int. J. Theor. Phys.* **52** 156–62

[25] Zeng G and Zhang W 2000 Identity verification in quantum key distribution *Phys. Rev.* A **61** 022303

[26] Lin S, Huang C and Liu X 2013 Multi-user quantum key distribution based on Bell states with mutual authentication *Phys. Scr.* **87** 035008

[27] Huang W, Xu B J, Duan J T, Liu B, Su Q, He Y H and Jia H Y 2016 Authenticated quantum key distribution with collective detection using single photons *Int. J. Theor. Phys.* **55** 4238–56

[28] Xin X, Hua X, Li C and Chen D 2016 Quantum authentication of classical messages using non- orthogonal qubits and Hash function. International journal of u-and e-service *Sci. Technol.* **9** 181–6

[29] Yuan H, Liu Y-M, Pan G-Z, Zhang G, Zhou J and Zhang Z-J 2014 Quantum identity authentication based on ping-pong technique without entanglements *Quantum Inf. Process.* **13** 2535–49

[30] Guan D-J, Wang Y-J and Zhuang E 2014 A practical protocol for three-party authenticated quantum key distribution *Quantum Inf. Process.* **13** 2355–74

[31] Yu K, Yang C, Liao C and Hwang T 2014 Authenticated semi-quantum key distribution protocol using Bell states *Quantum Inf. Process.* **13** 1457–65

[32] Meslouhi A and Hassouni Y 2017 Cryptanalysis on authenticated semi-quantum key distribution protocol using Bell states *Quantum Inf. Process.* **16** 18

[33] Luo Y-P, Chou W-H and Hwang T 2017 Comment on a practical protocol for three-party authenticated quantum key distribution *Quantum Inf. Process.* **16** 119

[34] Li C M, Yu K F, Kao S H and Hwang T 2016 Authenticated semi-quantum key distributions without classical channel *Quantum Inf. Process.* **15** 2881–93

[35] Lindell Y and Katz J 2014 *Introduction to Modern Cryptography* (Chapman and Hall/CRC)

[36] Li D, Zhang J, Guo F Z, Huang W, Wen Q Y and Chen H 2013 Discrete-time interacting quantum walks and quantum Hash schemes *Quantum Inf. Process.* **12** 1501–13

[37] Venegas-Andraca S E 2012 Quantum walks: a comprehensive review *Quantum Inf. Process.* **11** 1015–106

[38] Abd-El-Atty B 2023 Efficient S-box construction based on quantum-inspired quantum walks with PSO algorithm and its application to image cryptosystem *Complex Intell. Syst.* **9** 4817–35

[39] Yang Y G, Xu P, Yang R, Zhou Y H and Shi W M 2016 Quantum hash function and its application to privacy amplification in quantum key distribution, pseudo-random number generation and image encryption *Sci. Rep.* **6** 19788

[40] Li D, Yang Y G, Bi J L, Yuan J B and Xu J 2018 Controlled alternate quantum walks based quantum Hash function *Sci. Rep.* **8** 225

[41] Yang Y, Zhang Y, Xu G, Chen X, Zhou Y H and Shi W 2018 Improving the efficiency of quantum Hash function by dense coding of coin operators in discrete-time quantum walk *Sci. China Phys. Mech. Astron.* **61** 030312

[42] Yang Y G, Bi J L, Chen X B, Yuan Z, Zhou Y H and Shi W M 2018 Simple Hash function using discrete-time quantum walks *Quantum Inf. Process.* **17** 189

[43] EL-Latif A A A, Abd-El-Atty B, Venegas-Andraca S E and Mazurczyk W 2019 Efficient quantum-based security protocols for information sharing and data protection in 5G networks *Future Gener. Comput. Syst.* **100** 893–906

[44] Abd-El-Atty B, El-Latif A A A and Venegas-Andraca S E 2019 An encryption protocol for neqr images based on one-particle quantum walks on a circle *Quantum Inf. Process.* **18** 272

[45] El-Latif A A A, Abd-El-Atty B, Amin M and Iliyasu A M 2020 Quantum-inspired cascaded discrete-time quantum walks with induced chaotic dynamics and cryptographic applications *Sci. Rep.* **10** 1930

[46] El-Latif A A A, Abd-El-Atty B, Mazurczyk W, Fung C and Venegas-Andraca S E 2020 Secure data encryption based on quantum walks for 5G internet of things scenario *IEEE Trans. Netw. Service Manage.* **10** 1930

[47] Abd-El-Atty B and Abd EL-Latif A A 2023 Applicable image cryptosystem using bit-level permutation, particle swarm optimisation and quantum walks *Neural Comput. Appl.* **35** 18325–341

[48] Zhang W, Qiu D and Mateus P 2018 Security of a single-state semi-quantum key distribution protocol *Quantum Inf. Process.* **17** 1–21

[49] Krawec W 2015 Mediated semiquantum key distribution *Phys. Rev.* A **91** 032323

[50] Liu Z R and Hwang T 2018 Mediated semi-quantum key distribution without invoking quantum measurement *Ann. Phys., Lpz.* **530** 1700206

[51] Akerele M, Al-Anbagi I and Erol-Kantarci M 2019 A fiber-wireless sensor networks QoS mechanism for smart grid applications *IEEE Access* **7** 37601–610

[52] EL-Latif A A A, Abd-El-Atty B and Venegas-Andraca S E 2020 Controlled alternate quantum walk-based pseudo-random number generator and its application to quantum color image encryption *Physica* A **547** 123869

[53] Cabello A 2000 Quantum key distribution in the Holevo limit *Phys. Rev. Lett.* **85** 5635

[54] Shukla C, Thapliyal K and Pathak A 2017 Semi-quantum communication: protocols for key agreement, controlled secure direct communication and dialogue *Quantum Inf. Process.* **16** 295