Future Generation Computer Systems 100 (2019) 893–906

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Efficient quantum-based security protocols for information sharing and data protection in 5G networks

Ahmed A. Abd EL-Latif [a,b,*], Bassem Abd-El-Atty [a], Salvador E. Venegas-Andraca [c], Wojciech Mazurczyk [d]

[a] Mathematics and Computer Science Department, Faculty of Science, Menoufia University, Shebin El-Koom, Egypt
[b] School of Information Technology and Computer Science, Nile University, Egypt
[c] Tecnologico de Monterrey, Escuela de Ingenieria y Ciencias. Ave. Eugenio Garza Sada 2501, Monterrey, NL 64849, Mexico
[d] Institute of Telecommunications, Faculty of Electronics and Information Technology, Warsaw University of Technology, 15/19 Nowowiejska Str., 00-665 Warsaw, Poland

HIGHLIGHTS

- Two efficient hash function mechanisms for 5G applications were proposed.
- Two efficient security protocols for secure data in 5G network were proposed.
- Results show high security, efficiency, and robust against several attacks.

ARTICLE INFO

Article history:
Received 15 March 2019
Received in revised form 2 May 2019
Accepted 19 May 2019
Available online 30 May 2019

Keywords:
5G networks
Security protocols
Authentication
Quantum hash function
Quantum walks

ABSTRACT

Fifth generation (5G) networks aim at utilizing many promising communication technologies, such as Cloud Computing, Network Slicing, and Software Defined Networking. Supporting a massive number of connected devices with 5G advanced technologies and innovating new techniques will surely bring tremendous challenges for trust, security and privacy. Therefore, secure mechanisms and protocols are required as the basis for 5G networks to address this security challenges and follow security-by-design but also security-by-operations rules. In this context, new efficient cryptographic protocols and mechanisms are needed in order to design and achieve information sharing and data protection protocols in 5G networks. In the literature, several security schemes based on unproven assumptions of computational complexity and mathematical models were proposed. However, the cryptanalysis is able to break most of the existing proposals in the presence of several weakest links in the designs. Recently, quantum walks (QWs) have been introduced as an excellent mechanism for generating cryptographic keys due to its nonlinear chaotic dynamical performance, high sensitivity to initial control parameters, stability and very large key space theoretically strong enough to resist various known attacks. This paper firstly proposes two efficient hash function mechanisms for 5G networks applications based on QWs, namely QWHF-1 and QWHF-2. Then, based on these hash functions, two efficient security protocols for securing data in 5G network scenario are proposed. Performance analyses and simulation results show that the proposed approaches are characterized with high security, efficiency, and robustness against several well-known attacks which nominate them as excellent candidates for securing 5G applications.

1. Introduction

With the growth and vast progress of fourth generation (4G) networks, it is reasonable to expect that fifth generation (5G) networks will deliver a wide range of high-quality services [1]. It is envisioned that 5G networks will provide significantly higher data bandwidth and massive networking capacities resulting in unfaltering user experiences. Internet of Things (IoT) has been protruding as an integrated part of 5G networks [2–12] , which considers a concept reflecting a connected set of anything, anyone, anyplace, anytime, any service, and any network. In the context of 5G networks, IoT devices are becoming active players with capabilities to communicate and interact with heterogeneous devices, sensors, services, applications, data providers and IoT-enabled ecosystems. IoT aims at integrating the physical and

* Corresponding author at: Mathematics and Computer Science Department, Faculty of Science, Menoufia University, Shebin El-Koom, Egypt.
E-mail addresses: a.rahiem@gmail.com, alatif@science.menofia.edu.eg, AAbdelLatif@nu.edu.eg (A.A.A. EL-Latif), bassimeldeeb@gmail.com (B. Abd-El-Atty), salvador.venegas-andraca@keble.oxon.org, svenegas@tec.mx (S.E. Venegas-Andraca), w.mazurczyk@tele.pw.edu.pl (W. Mazurczyk).

https://doi.org/10.1016/j.future.2019.05.053
0167-739X/

virtual worlds using 5G networks as a medium to communicate and exchange information.

5G networks are envisioned to have a central role in our daily life. Moreover, 5G networks aim at combining many promising network technologies such as Software Defined Networking (SDN), Network Functions Virtualization (NFV), Information-Centric Network (ICN), Network Slicing, and Cloud Computing, among others. On the one hand, this can be seen as a great opportunity for improvements while on the other hand such integration can result in new, enormous privacy and security challenges for 5G networks [13–23] . Therefore, secure network architectures and authenticated protocols are required as the basis for 5G networks to address security and privacy problems and follow not only security-by-design but also security-by-operations rules [24–27].

If devices in the network do not verify their counterpart's identity, eavesdroppers will be able to perform active attacks such as man-in-the-middle and impersonation attacks. This means that an eavesdropper Eve is able to impersonate Alice (Bob) to communicate with Bob (Alice). Thereby, Eve can have full access to the confidential information that has been transmitted between Alice and Bob without being noticed at all. A solution to this problem is using hash functions to guarantee the integrity and origin of the transmitted message. In general, hash functions are hard to reconstruct for unknown inputs, hence their corresponding mathematical and computational complexity [28–32] constitute a central component in the authentication processes to guarantee the security of established communication channels [33–38].

Several authentication protocols and data security mechanisms designed for 5G networks that have been recently proposed [39–47] are based on mathematical conjectures and empirically estimated computational complexity functions. However, with the evolution of quantum technologies, some traditional hash functions, security mechanisms, and authentication protocols may be broken using quantum computer technology [48–50].

Inspired by the limitations of classical hash functions and the potential advantages of quantum computation, it is reasonable to expect quantum-based proposals of cryptosystems to achieve information sharing and data protection for 5G networks. The main contribution of this paper is to open the door towards using the capabilities of quantum technologies in 5G networks.

Among the computational paradigms developed in quantum computation, we find quantum walks (QWs), a universal model of quantum computation that has some nonlinear properties, together with high sensitivity to initial control parameters, that can be used to produce chaotic dynamical behavior and, consequently, may be employed as a source to produce keys for cryptographic protocols [49,51].

Let us now describe the contents of this paper. Firstly, an analysis of the existing quantum hash function (QHF) schemes [50, 52–55] utilizing QWs is presented. Based on the limitations identified in these hash functions, a modified version, namely QWHF-1, is presented. Then, a novel quantum hash function based on quantum walks, namely QWHF-2, is proposed. Using QWHF-1, an efficient authenticated key distribution (AKD) protocol utilized in encrypting and sharing the data stored in cloud servers of 5G networks is proposed. While based on QWHF-2, an efficient authenticated quantum direct communication (AQDC) protocol for device-to-device (D2D) communications for 5G networks is introduced. The proposed AKD protocol has several advantages such as defenses against various kinds of known attacks and its security provided by quantum properties. The AQDC is able to utilize all transmitted photons to encode secret messages and their corresponding hash values. Several tests and security analysis are provided to prove the efficiency of the proposed approaches in terms of performance and security analysis. Results show the robustness of proposed mechanisms against most well-known attacks for the cryptosystem applications.

This work is organized and ordered as follows: the proposed framework for 5G networks based on quantum technologies is given in Section 2. Section 3 is devoted to the theoretical background of quantum walks. Section 4 analyzes existing QHF schemes and introduces the modified quantum hash function version based on the controlled alternate quantum walks, namely QWHF-1, as well as the second quantum hash function, QWHF-2. Section 5 is focused on the novel authentication mechanisms based on the proposed hash function schemes presented in Section 4. Section 6 is devoted to presentation of the experimental results and analysis of the proposed QWHF approaches. Section 7 gives the security analysis of the proposed authentication protocols. Finally, Section 8 concludes our work.

2. Proposed framework for 5G networks based on quantum technologies

Providing secure authentication and data transmission mechanisms for the connected devices in 5G networks are required. Inspired by the limitations of current cryptosystems and the advantages of quantum technology, new constructions of cryptosystems techniques are designed in order to achieve information sharing and data protection for 5G networks.

Here, we propose an efficient AKD protocol utilized to encrypt and share data stored in cloud servers of 5G networks. In addition, we design an efficient AQDC protocol for D2D communications by utilizing the benefits of quantum walks. The proposed framework for 5G networks based on quantum technologies is given in Fig. 1. It enables IoT devices to communicate with each other's via AQDC protocol and enable IoT devices to store and share their data by utilizing the AKD protocol to encrypt the data before storing it in the cloud storage. The proposed protocols have several advantages such as defenses against various kinds of known attacks and its security guaranteed by quantum properties.

3. Theoretical background of quantum walks

Quantum walks, a generalization of random walks in the quantum domain, are tools for developing quantum algorithms that also constitute universal models of quantum computation [56,57]. Quantum walks can be either continuous or discrete models of computation, depending on how time is measured ($t \in \mathbb{R}^+ \cup \{0\}$ for the continuous case and $t \in \mathbb{N} \cup \{0\}$ for the discrete case). In both cases and so far, the mathematical and computational properties of quantum walks have been studied on graphs. In this paper, we focus on the discrete-time quantum walk model which we use to construct quantum hash functions to design the proposed security mechanisms for 5G networks.

The elements of a coined discrete quantum walk are a coin, a walker, evolution operators and a set of observables. A walker is a quantum system living in a Hilbert space $\#(\mathcal{H}_p) = N$ if it runs on a circle of N vertices. The coin is typically a quantum system living in a two-dimensional Hilbert space $\mathcal{H}_c$. The total state of a discrete quantum walk lives in $\mathcal{H}_p \otimes \mathcal{H}_c$.

The total evolution operator $\hat{U}$ for a discrete quantum walk is given by Eq. (1):

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

Here, $\hat{S}$ refers to the shift operator acting on a circle with N vertices which can be described as

$$\hat{S} = \sum_{x}^{N} (|(x+1) \ \ mod\ N, 0\rangle\langle x, 0| + |(x-1) \ \ mod\ N, 1\rangle\langle x, 1|) \tag{2}$$

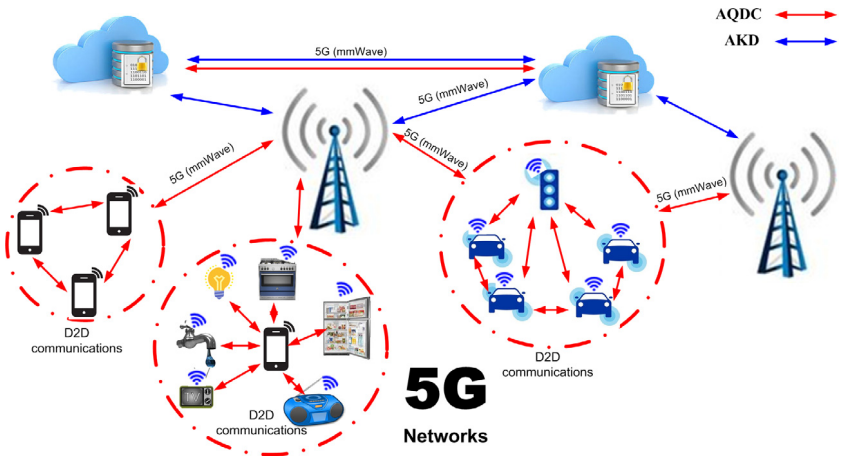


Fig. 1. The proposed framework for the 5G networks based on quantum technologies.

The operator $\hat{C}$ refers to the coin operator and can be defined in matrix notation as

$$C = \begin{pmatrix} \cos\ \theta & \sin\ \theta \\ \sin\ \theta & -\cos\ \theta \end{pmatrix} \tag{3}$$

After n steps the final state of the system $|\varphi\rangle_n$ can be expressed as

$$|\varphi\rangle_n = \left(\hat{U}\right)^n |\varphi\rangle_0 \tag{4}$$

The probability of finding the particle at position x after n steps is given by

$$P(x, n) = \sum_{c\in\{0,1\}} |\langle x, c| \left(\hat{U}\right)^n |\varphi\rangle_0|^2 \tag{5}$$

Furthermore, note that the probability $P(x, n)$ has non-zero value in any position x, if the number of running steps n is greater than or equal to the number of vertices N [50].

4. Quantum Hash function schemes

4.1. Existing QHF schemes and their analysis

Quantum walks can be thought of as non-linear mappings $Q : \mathcal{H} \mapsto \mathcal{P}$ where $\mathcal{H}$ is a Hilbert space in which the quantum walker lives and $\mathcal{P}$ is a set of probability distributions. This property, together with high sensitivity and other characteristics, allow us to think of quantum walks as chaotic systems [56–59]. Thus, quantum walks can be used for producing quantum hash functions as in [50,52–55]. In [50], Li et al. presented the first QHF based on one-dimensional two-particle quantum walks and Yang et al. [52] utilized this QHF [50] to present some applications in pseudo-random number generator, privacy amplification process of quantum key distribution, and image encryption. In [53], Li et al. proposed a QHF based on CAQWs on a circle with N vertices. At each step of a CAQW controlled by a binary message m, the evolution operator $\hat{U}_0$ ($\hat{U}_1$) is applied on the whole quantum system $|\varphi\rangle$ when the nth-*bit* of m is 0 (1).

$$\begin{aligned} \hat{U}_0 &= \hat{S}_y(\hat{I} \otimes \hat{C}_0)\hat{S}_x(\hat{I} \otimes \hat{C}_0) \\ \hat{U}_1 &= \hat{S}_y(\hat{I} \otimes \hat{C}_1)\hat{S}_x(\hat{I} \otimes \hat{C}_1) \end{aligned} \tag{6}$$

Here, $\hat{S}_y$ refers to the shift operator running on y dimensional and can be defined as follows.

$$\hat{S}_y = \sum_{x,y}^{N} (|x, (y+1)\ \ mod\ N, 0\rangle\langle x, y, 0| + |x, (y-1)\ \ mod\ N, 1\rangle\langle x, y, 1|) \tag{7}$$

Also $\hat{S}_x$ can be defined as $\hat{S}_y$, which is running on x dimensional.

One of the main benefits of QHFs based on QWs is that the length of the hash value changes with respect to the number of vertices N in the circle. Moreover, it is helpful to develop various applications for 5G networks. However, if the length of the bit string of the message is less than the number of nodes N, the system will be inefficient as some positions have zero possibilities. Quantum walk-based QHFs presented in [50,52–55] exhibit this limitation. In Section 4.2, we solve this issue by adding a new coin operator to the QHF presented in [53] in order to overcome this constraint.

4.2. The modified alternate quantum walks based quantum hash function (QWHF-1)

In the modified QWHF-1, we use three coin operators $\hat{C}_0$, $\hat{C}_1$ and $\hat{C}_2$ to build corresponding evolution operators $\hat{U}_0$, $\hat{U}_1$ and $\hat{U}_2$. Operators $\hat{U}_0$ or $\hat{U}_1$ depending on the value of the *nth* bit of m is *"0"* or *"1"*, respectively and operator $\hat{U}_2$ are applied when the *nth* step exceeds the length of m and does not reach N (the number of vertices in the circle).

The steps for constructing the modified QHF are indicated below.

1. Select initial values for the key parameters $(N, \alpha, \theta_0, \theta_1, \theta_2)$ for running CAQWs on a circle with N vertices controlled by binary message m for generating a probability distribution matrix P with size $N\times N$ [49,59]. The initial state of the coin particle is $|\text{coin}\rangle = \cos\alpha|0\rangle + \sin\alpha|1\rangle$ while θ_0, θ_1 and θ_2 are parameters to construct coin operators $\hat{C}_0$, $\hat{C}_1$ and $\hat{C}_2$, respectively.
2. Compute the hash value for the binary message m by converting the probability matrix P to a bit string as follows:

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

where the length of bit hash value is $8N^2$.

4.3. The proposed QWHF-2

To construct QWHF-2, we use two coin operators $\hat{C}$ and $\hat{C}_0$. The first coin $\hat{C}$ is constructed by θ, where θ is the ASCII-code for the nth character of the message, and the second coin $\hat{C}_0$ is applied when the nth step exceeds to the length of the message and does not reach N. The steps for constructing this QHF are indicated below.

1. Choose initial values for the parameters (N, α, θ_0).
2. Run one-dimensional one-particle QWs on a circle with N vertices, to generate a probability distribution P with the size N under the control of message m, where the initial state of coin particle is $|\text{coin}\rangle = \alpha|0\rangle + \beta|1\rangle$ and θ_0 is the parameter of coin operator $\hat{C}_0$.
3. Construct a hash value for message m by converting the probability matrix P to a bit string as stated in Eq. (8), where the length of the hash value is $8N$.

5. Security protocols for 5G networks based on proposed QHFs

5.1. The proposed AKD protocol based on QWHF-1

The central problem of symmetric cryptographic algorithms is keystream generation and distribution. The sender and the receiver need to share with each other a secure keystream for encryption and decryption process. It requires that the sender (Alice) finds some secure communication channel to establish a keystream to the receiver (Bob) [60].

Based on the properties of quantum mechanics, we present an authenticated key distribution protocol based on CAQWs which is designed to establish a keystream between two participants. The proposed protocol requires pre-shared master key parameters. The procedure of the proposed protocol are illustrated in Fig. 2 and is formulated in the following steps.

1. The sender (Alice) announces publicly with the receiver (Bob) an integer odd number N_p, for running CAQWs (N_p, α, θ_2) in order to generate a hash value $B \in \{0,1\}^{8N_p^2}$ with the length $8 \times N_p^2$.
2. Alice sends to Bob a sequence of random bits $S \in \{0,1\}^*$ with the length less than or equal to the length of B and stores only the corresponding bit values of ith-bit of S when ith-bit of B is *"0"* as $R \in \{0,1\}^x$.
3. Upon receiving the bit sequence S, Bob stores only the ith-bit of S when ith-bit of B is *"0"* as bit string $R \in \{0,1\}^x$.
4. Alice announces publicly with Bob an integer odd number N_c, in order to run CAQWs $(N_c, R, \alpha, \theta_0, \theta_1, \theta_2)$ for generating a bit string $K_c \in \{0,1\}^{8N_c^2}$ with the length $8 \times N_c^2$.
5. In order to detect any eavesdropping activity, Alice selects and announces with Bob the first $4 \times N_c^2$-*bit* of K_c sequence. If the compared results are the same, Bob announces the remaining bits of K_c to be checked by Alice. Thereby, both participants Alice and Bob authenticate each other. If there is any error, both participants terminate the protocol.
6. Finally, Alice announces publicly with Bob an integer odd number N_k, in order to run CAQWs $(N_k, R, \alpha, \theta_0, \theta_1, \theta_2)$ for generating a hash value $K \in \{0,1\}^{8N_k^2}$ as a secret key with length $8 \times N_k^2$ bit.

From the information published via the communication channel about the hash values constructed by CAQWs, no one is able to infer any information about the master key parameters $(\alpha, \theta_0, \theta_1, \theta_2)$ used for constructing these values or the final secret key K. Therefore, the master key may be reused if needed. Furthermore, both legitimate participants can share several secret keys using the same shared bits by repeating the *step 6* of the protocol several times with announcing different N_k to conform to various applications of 5G networks. Fig. 3 presents an example of this rationale.

5.2. The proposed AQDC based on QWHF-2

In quantum protocols, there are two ways for enabling communication between participants and they mainly involve single photons and entangled states. A single photon carries classical/quantum information via a quantum channel. There are many kinds of entangled states, such as Einstein–Podolsky–Rosen (EPR) pairs, Greenberger–Horne–Zeilinger (GHZ), cluster states, W states and χ-type states, where EPR pairs are widely used [61]. Single photons become one of the ideal information carriers in the field of quantum communication, which are easy to implement, simple to operate, and highly efficient without sacrificing security.

Message authentication aims at verifying the integrity and origin of the transmitted message after it reaches the receiver (Bob).

In [62], Luo et al. presented two AQDC schemes using Bell states to transmit a secret message with the length n, both schemes require a pre-shared secret key with the length $12 \times n$. Almousa et al. [63] improved the protocols introduced in [62] using a keyed hash function instead of the pre-shared key, where the participants share the key for the hash function and its output length. Since the advent of quantum computing technology may defy the robustness of some hash functions [48–50], here we present a new AQDC protocol using single photons based on quantum hash function instead of classical hash functions.

We now introduce notation and encoding rule for our proposed AQDC protocol. Classical bits can be implemented using single photon polarization. The linear polarization of a photon (Z-basis) is distinguished by the vertical and horizontal polarizations, which can be assigned to 1 and 0, respectively.

$$|V\rangle = |1\rangle \tag{9}$$

$$|H\rangle = |0\rangle \tag{10}$$

The superposition of the two types of linear polarized states will produce various photon states in direction of $+45°$ and $+135°(-45°)$(X-basis), which can be assigned to 0 and 1, respectively.

$$|+\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \tag{11}$$

$$|-\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{12}$$

To represent classical bit 0, the state $|0\rangle$ or $|+\rangle$ is used. Also, state $|1\rangle$ or $|-\rangle$ are used to represent the classical bit 1. So, to represent any classical bit string, we must first decide the encoding bases (Z-basis, X-basis) we shall use. The details of the communication processes of the proposed AQDC protocol based on single photons and the QWHF-2 are illustrated in Fig. 4.

The specific steps of this protocol are described as follows:

Step 1: The sender (Alice) shares with the receiver (Bob) the parameters (N, α, θ_0) for running the proposed QHF (QWHF-2).

Step 2: Alice gets the hash value v_1 for the secret message $QHF\ (secret\ message) = b_1 b_2 \ldots b_v$, and then gets the hash value v_2 for v_1 $QHF\ (v_1) = h_1 h_2 \ldots h_v$.

Step 3: Alice converts the secret message into bit string $\mathrm{m} = m_1 m_2 \ldots m_n$, then executes the exclusive-OR operation by blocks to the bit string $\mathrm{m} = m_1 m_2 \ldots m_n$ and the hash value v_2 $(h_1 h_2 \ldots h_v)$.

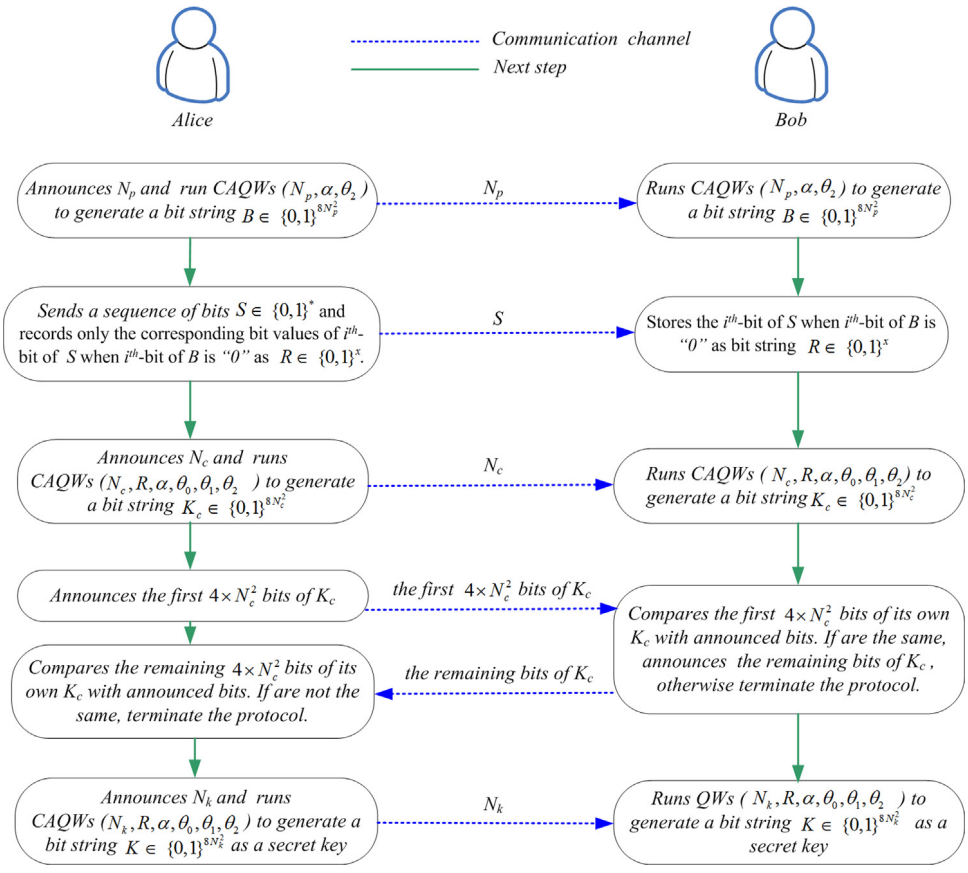


Fig. 2. The proposed AKD protocol for which the length of the shared final key depends only on the announced N_k and not on the number of exchanged bits to conform to various applications of 5G networks.

$$\mathrm{m} \oplus \mathrm{v}_2 = \overbrace{m_1 m_2 \ldots m_v}^{h_1 h_2 \ldots h_v \oplus} \overbrace{m_{1+v} m_{2+v} \ldots m_{v+v}}^{h_1 h_2 \ldots h_v \oplus} \ldots \overbrace{m_i m_{i+1} \ldots m_n}^{h_1 h_2 \ldots h_v \oplus} = b_1 b_2 \ldots b_n$$

Step 4: Alice runs the QHF with no message and gets the hash value as $k\ QHF\ () = k_1 k_2 \ldots k_v$.

Step 5: Alice generates a sequence of single photons S according to B sequence $\mathrm{B} = (\mathrm{m} \oplus \mathrm{v}_2, \mathrm{v}_1) = b_1 b_2 \ldots \overbrace{b_n b_{1+n} b_{2+n} \ldots b_{v+n}}^{k}$ and K ($K = \overbrace{k_1 k_2 \ldots k_v}^{k} \overbrace{k_{1+v} k_{2+v} \ldots k_{v+v}}^{k} \ldots \overbrace{\ldots k_{n-1} k_n}^{k}$) as follows. Qubits are prepared according to the following rule: If the ith bit of K is 0, then Alice produces the qubit S_i in Z-basis as $|0\rangle(|1\rangle)$ according to the bit B_i. On the contrary, if the ith bit of K is 1, then Alice produces the qubit S_i in X-basis as $|+\rangle(|-\rangle)$.

Step 6: Alice sends the photon sequence S to Bob via the quantum channel.

Step 7: Upon receiving the photon sequence, Bob measures the qubits in basis (Z- basis or X- basis) according to $K\ \ QHF\ () = k_1 k_2 \ldots k_v$ to obtain the bit sequence B'.

Step 8: Bob extracts from B' the hash code $v_1' = b'_{1+n} b'_{2+n} \ldots b'_{n+v}$ and $b' = b'_1 b'_2 \ldots b'_n$, then gets the hash value v_3 for v_1' $QHF\ (v_1') = h_1 h_2 \ldots h_v$.

Step 9: Bob executes the exclusive-OR operation by blocks to the bit sequence b' and the hash value v_3 to obtain the bit string $\mathrm{m}' = m'_1 m'_2 \ldots m'_n$.

$$\mathrm{m}' = \overbrace{b'_1 b'_2 \ldots b'_v}^{h_1 h_2 \ldots h_v \oplus} \overbrace{b'_{1+v} b'_{2+v} \ldots b'_{v+v}}^{h_1 h_2 \ldots h_v \oplus} \ldots \overbrace{\ldots b'_{n-1} b'_n}^{h_1 h_2 \ldots h_v \oplus} = m'_1 m'_2 \ldots m'_n$$

Step 10: Bob converts the bit string $\mathrm{m}' = m'_1 m'_2 \ldots m'_n$ to the string message and gets the hash value v_4 for the recovered message $QHF\ (recovered\ message) = b_1 b_2 \ldots b_v$.

Step 11: Bob checks the hash code v_1' obtained from the bit sequence B' with the hash value v_4 for the recovered message. If the two hash values are the same, then the connection is secure, otherwise the connection is considered as insecure and it is disconnected.

6. Experimental analysis and results for QWHFs

We have run several test analyses to evaluate the performance of the proposed quantum hash functions, including sensitivity analysis of the generated hash values, statistical analysis of confusion and diffusion, and uniform distribution on hash space. In this section, we present our results.

6.1. Initial values of the utilized parameters

The initial values used to run CAQWs on a circle to generate the hash value for QWHF-1 are N=5, α=0, $\theta_0 = \pi/6$, $\theta_1 = \pi/3$, and $\theta_2 = \pi/4$. On the other hand, the initial values for running QWs on a circle to generate the hash value for QWHF-2 are N=25, α=0, β=0, and $\theta_0 = \pi/4$.

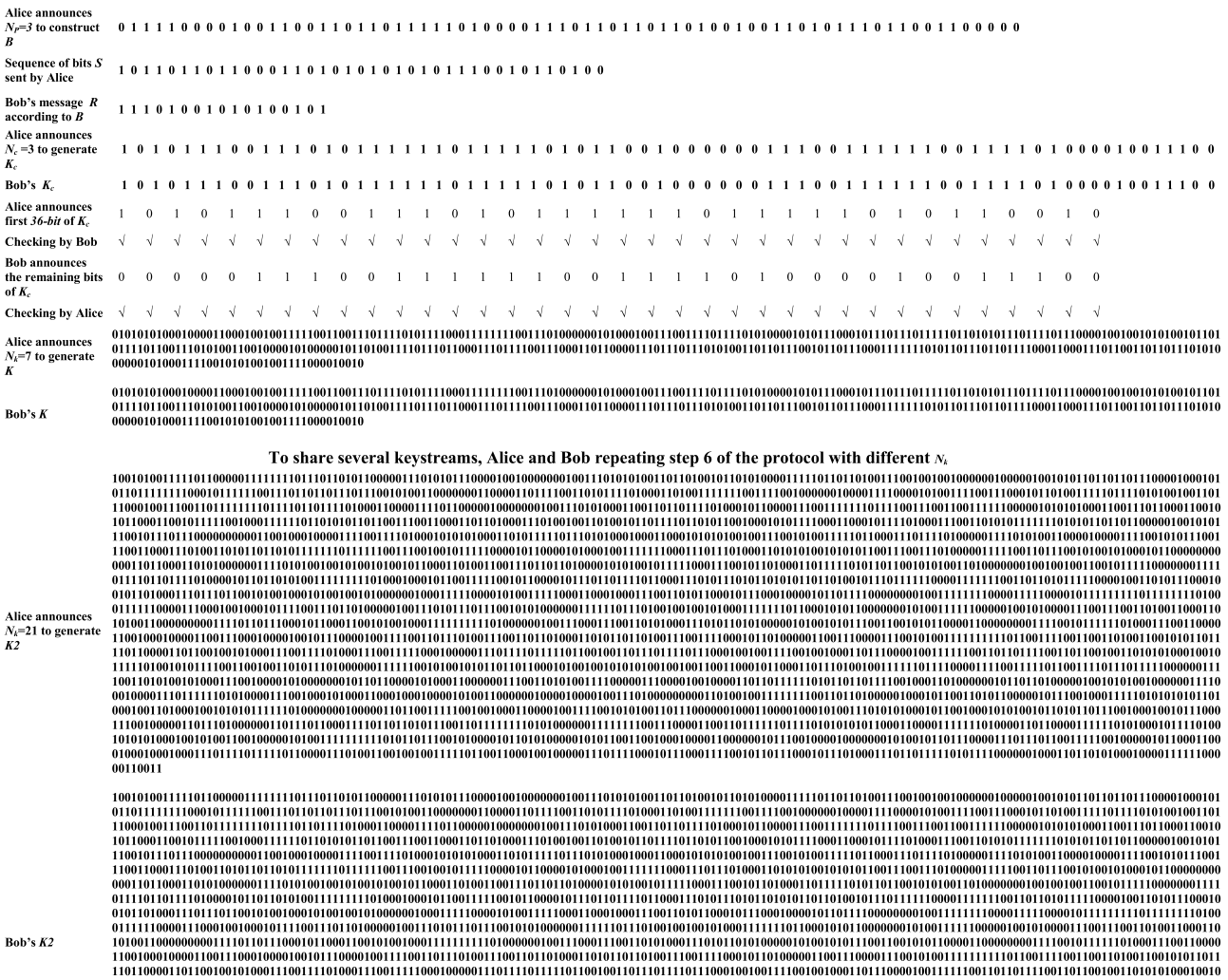


Fig. 3. An illustrative example for the proposed authenticated key distribution protocol, where the pre-shared master key parameters are α = 0, $\theta_0 = 45°$, $\theta_1 = 30°$, and $\theta_2 = 55°$.

6.2. Sensitivity analysis of the generated hash values

6.2.1. QWHF-1

To show the sensitivity of the QWHF-1 to tiny modifications of the message, we use the original message with its tiny modifications as listed below.

M1: "1011 0101 1101 0001 1010 1111"
M2: "0011 0101 1101 0001 1010 1111"
M3: "1111 0101 1101 0001 1010 1111"
M4: "1011 0101 1101 0001 1010 1110"
M5: "1011 0101 1101 0001 1010 1111 0"
M6: "1011 0101 1101 0001 1010 111"
M7: "10"

The corresponding hash values in a hexadecimal format are stated as follows:

QHF(M1): D93720CF6D39E81FD51E88417B97613FB64664F69AE73C368E
QHF(M2): 50436D4B180D64651F316350FAD7B9F35550DF2CB6656B6D97
QHF(M3): FB9E157F0BA65AE756FD80F23720F0DDE9C4386E50CD23F563
QHF(M4): 6C3F601E0B11A2C10A6131EDC343A1D2B12089C3FA8A4C6EEE
QHF(M5): 292D361F61E84F17E5397460412E01ADF3DA34D5353835987B
QHF(M6): 26EAAB7F0C01E29C1650A60629278E0E1F1C742F967501B88E
QHF(M7): FC1D409B8AE52103535C25FBC6F58DB1E537BA24E3E4AEC276

It is clear from Fig. 5 that any tiny changes of the original message will cause significantly different results in the final hash value. Also, it is clear from M7 that the modified QHF is efficient although the length of the message is less than the number of vertices N in the circle.

6.2.2. QWHF-2

To show the sensitivity of the proposed QWHF-2 to tiny changes of the used string, we use the message 'Quantum Hash Function' with its tiny modifications as listed below. Note that the message length is less than the number of vertices N in the circle (N=25).

S1: Quantum Hash Function
S2: Quantum Hash function
S3: Quantum hash Function

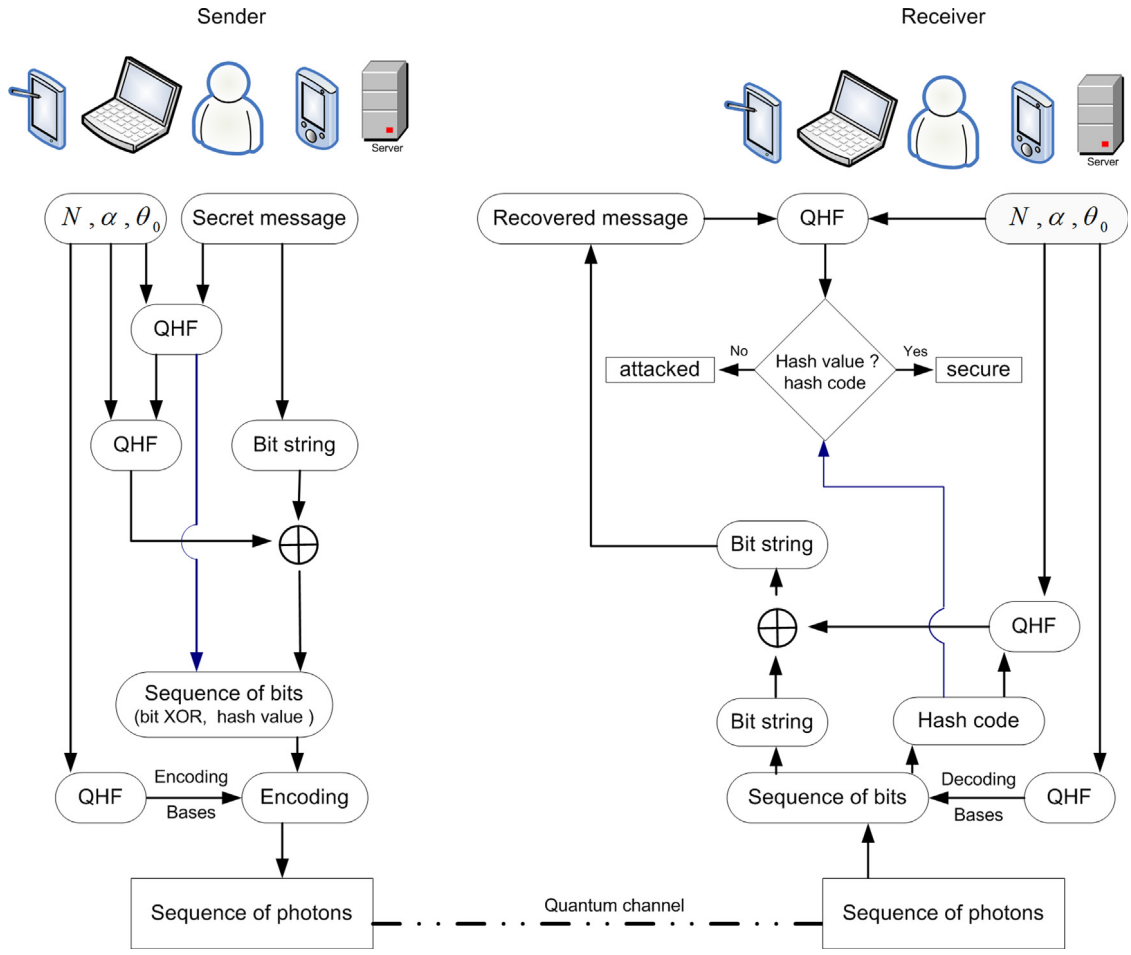


Fig. 4. The proposed AQDC protocol for transmitting and authenticating messages, which is based on single photons as a communication channel and the proposed QWHF-2.

S4: quantum Hash Function
S5: Quantum hash function
S6: Quantum Hash Functions
S7: Q

The corresponding hash values in the hexadecimal format are stated as follows:

QHF(S1): 75161C910606702D4900E500A61B05FBD4CF0E137E7702E387
QHF(S2): 2DB2E7F50D91D9683005EA001919BDA5B79ADF130A54AB0F4D
QHF(S3): C8AEBB8DA3AAB1013D032A03F2B4470A66C2EC4C51B7F9CFA2
QHF(S4): 64331D2633D5900B77307305A61677CAA6F1EE4351E200C698
QHF(S5): 6FFC4DCF26D76484041BB603C1CBE19F521F958363758FE7CD
QHF(S6): 54F533FB58BCF0838E006C00EF09E99AB4D65DBF2163B9C0DE
QHF(S7): 804512AC361F9189D3DCBF26EEE2CB2B851193FB29CFA08169

Fig. 6 presents additional data regarding the sensitivity of our protocol to small changes in its input.

6.3. Statistical analysis of the confusion and diffusion

Confusion and diffusion tests are run according to the following steps:

Step 1: Choose a message and generate its hash value.

Step 2: Change randomly one bit/char of the selected message and generate its new hash value.

Step 3: Count the different bits between the two hash values D_i.

Step 4: Repeat the above three steps T times.

Give the following definitions to test the performance of confusion and diffusion analysis.

Minimum of $D_i : D_{\min} = \min\left(\{D_i\}_1^T\right)$

Maximum of $D_i : D_{\max} = \max\left(\{D_i\}_1^T\right)$

Mean of $D_i : \bar{D} = \sum_{i=1}^{T} D_i/T$

Mean probability of $D_i : P = \left(\bar{D}/200\right) \times 100\%$

Standard variance of $D_i : \Delta D = \sqrt{\frac{1}{N-1}\sum_{i=1}^{T}\left(D_i - \bar{D}\right)^2}$

Tests were performed with T = 1000, 2000, 4000, 10000, respectively for both QWHFs and results are presented in Tables 1 and 2 for QWHF-1 and QWHF-2, respectively. We can see that the mean change probability P is roughly 50% and ΔD is very small, while D_{min} and D_{max} are around 100. Figs. 7 and 8 show the distribution of the number of the changed bits D_i and its histogram for QWHF-1 and T = 10000. Also, Figs. 9 and 10 present the distribution of the number of the changed bits D_i and its histogram for QWHF-2 and T = 10000. Thus, our results demonstrate the stability of confusion and diffusion tests for both QWHFs.

6.4. Uniform distribution on hash space

To investigate whether elements in hash space are uniformly distributed, we execute the steps of confusion and diffusion analyses from the previous subsection for T = 10000, then count the number of bits changed for each location. The distribution results on hash space for QWHF-1 are shown in Fig. 11, where

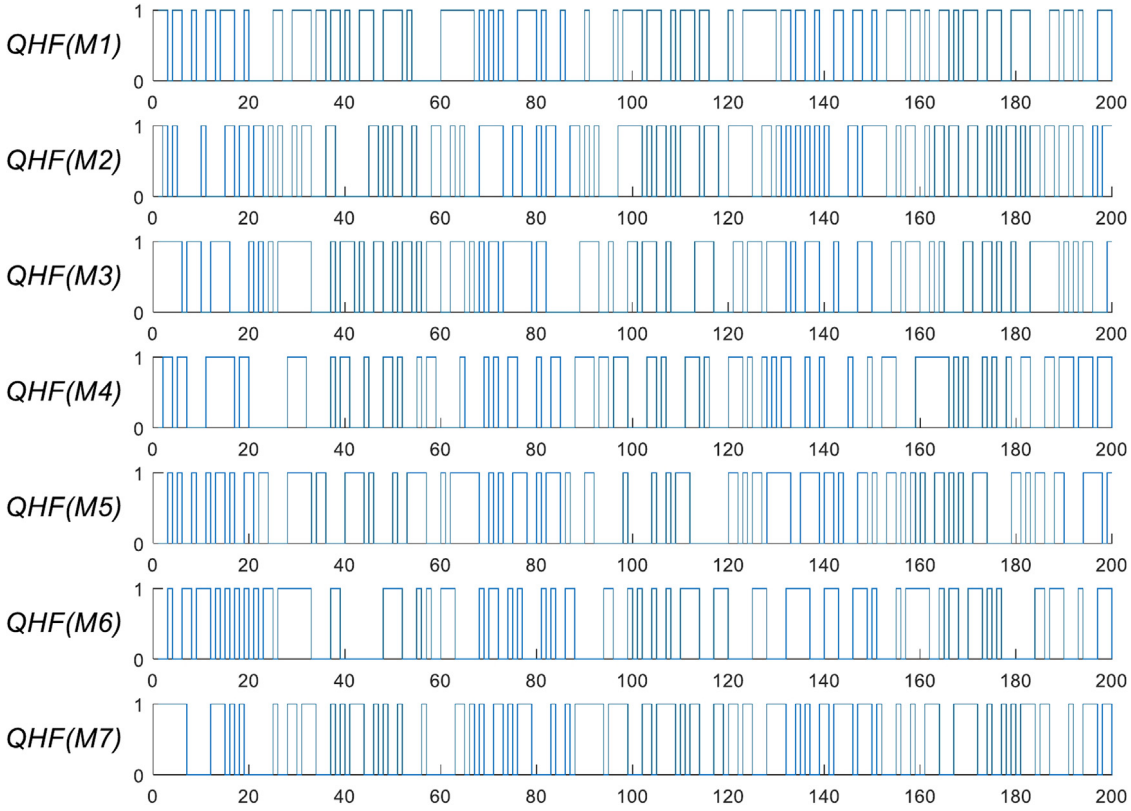


Fig. 5. 200-bit hash values for QWHF-1 for several messages.

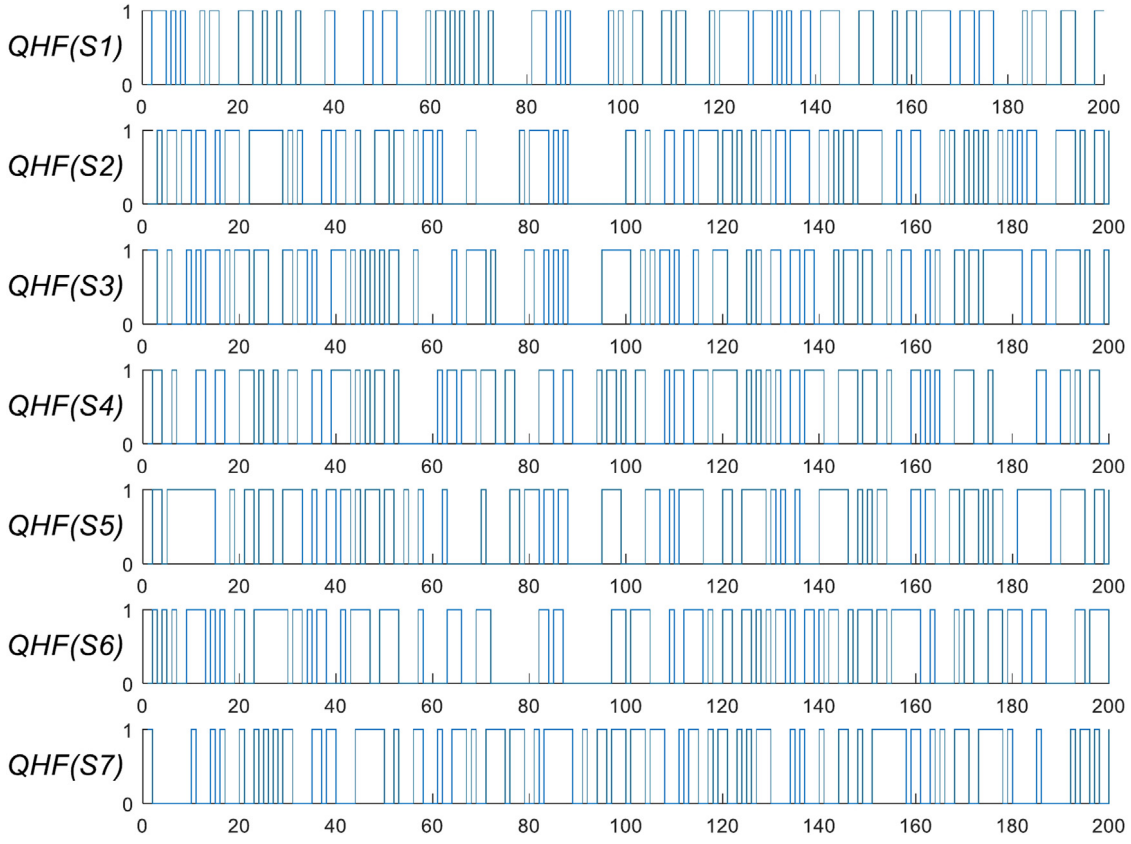


Fig. 6. 200-bit hash values for QWHF-2 for several messages.

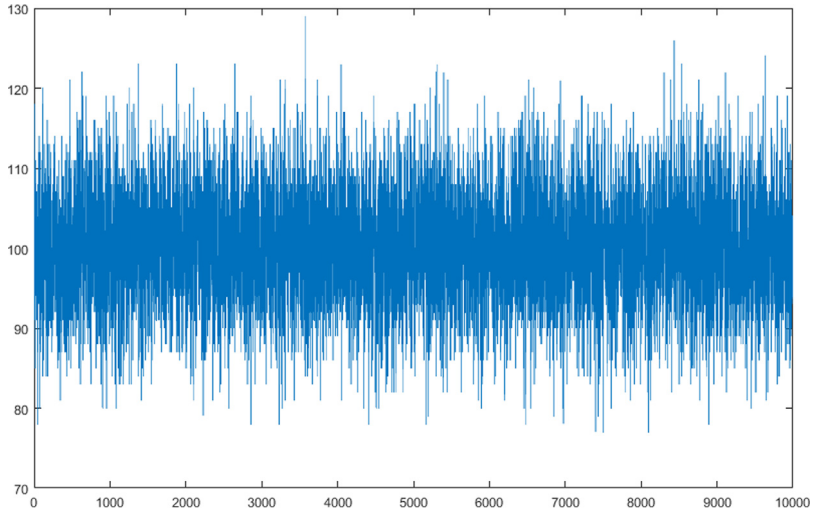


Fig. 7. The distribution of the number of changed bits D_i for QWHF-1 and T = 10000.

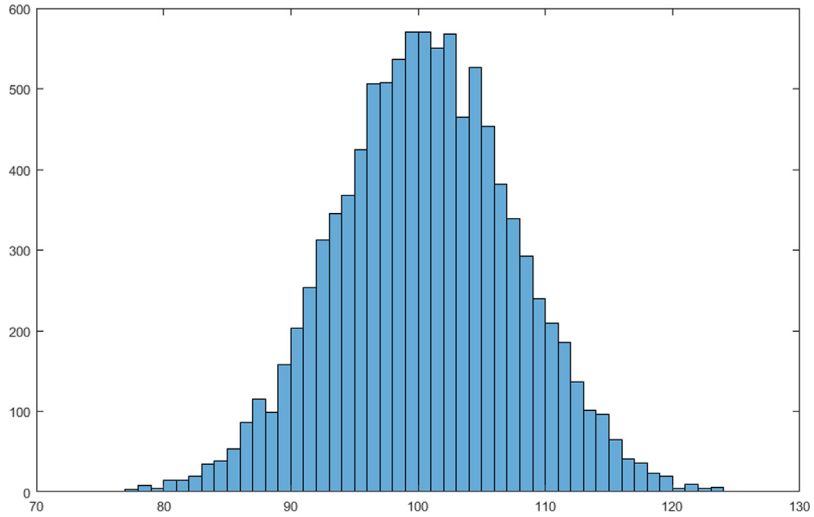


Fig. 8. The histogram of the number of changed bits D_i for QWHF-1 and T = 10000.

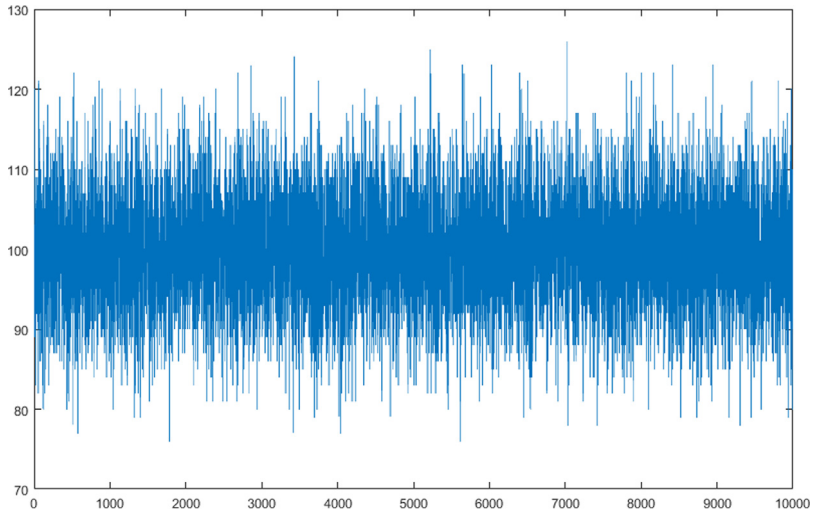


Fig. 9. The distribution of the number of changed bits D_i for QWHF-2 and T = 10000.

the maximum and minimum numbers of changed bits are 5131 and 4875 respectively, and the mean number of changed bits is 5005.35 that is close to the half of the test times. Also, distribution results on hash space for QWHF-2 are presented in Fig. 12. It

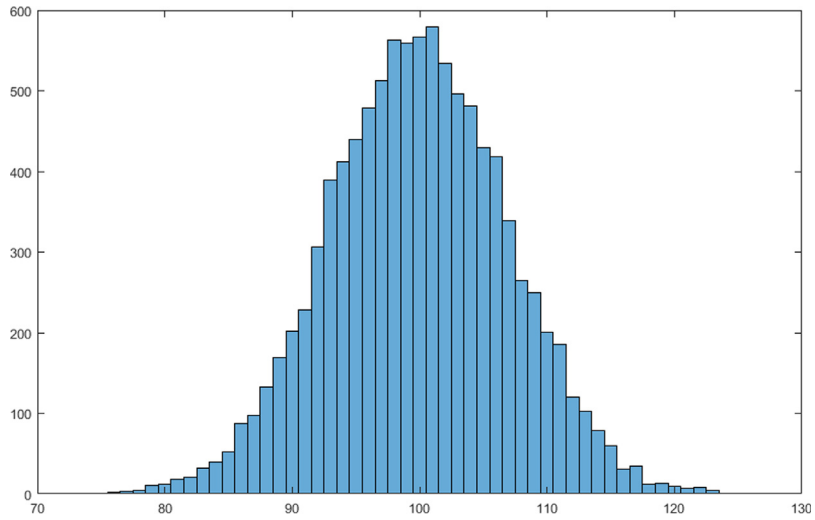


Fig. 10. The histogram of the number of changed bits D_i for QWHF-2 and T = 10000.

Table 1
The results of the confusion and diffusion tests for QWHF-1.

T	1000	2000	4000	10000
$D_{\min}$	78	77	77	77
$D_{\max}$	129	123	126	129
$\bar{D}$	100.3180	100.0395	100.0138	100.1070
P	50.1590	50.0198	50.0069	50.0535
ΔD	7.1189	7.2315	7.1192	7.0796

Table 2
The results of the confusion and diffusion tests for QWHF-2.

N	1000	2000	4000	10000
$D_{\min}$	78	78	76	76
$D_{\max}$	123	125	125	126
$\bar{D}$	100.1790	100.1475	100.0928	100.0380
P	50.0895	50.0737	50.0464	50.0190
ΔD	7.1276	7.1150	7.0103	7.1162

must be noted that the maximum and minimum numbers of changed bits are 5144 and 4839, respectively and the mean number of the changed bits is 5001.84 that is very close to the half of the test times. Furthermore, graphs presented in Figs. 11 and 12 provide experimental evidence of hash values being uniformly distributed in hash space. Therefore, modified QWHF-1 and proposed QWHF-2 are resistant against statistical attack.

6.5. Illustrative example

This section gives an illustrative example for computing the hash values in QHF [53], QWHF-1, and QWHF-2. Suppose, m is *"1"* and N is *5*.

1. for QHF in [53], the final state can be expressed as
$$|\varphi\rangle_{final} = \hat{U}_1|\varphi\rangle_0 \tag{13}$$
2. the final state for QWHF-1 can be expressed as
$$|\varphi\rangle_{final} = \hat{U}_2\hat{U}_2\hat{U}_2\hat{U}_2\hat{U}_1|\varphi\rangle_0 \tag{14}$$
3. the final state for QWHF-2 can be expressed as
$$|\varphi\rangle_{final} = \hat{U}_0\hat{U}_0\hat{U}_0\hat{U}_0\hat{U}|\varphi\rangle_0 \tag{15}$$

where the probability P has zero probability in some positions. The corresponding hash values in the binary format are given in Fig. 13 utilizing the same parameters. Likewise, the hash values are given in hexadecimal format as follows.

QWHF-1: 5A6E813431D1FB91EAF7584936AC1C7CEC0A8F9384534C763B
QWHF-2: 86DEA2995E
QHF [53]: 0000000000003F003F000000000000003F003F000000000000

Furthermore, the proposed authenticated key distribution protocol cannot be designed with the presented QHF in [53], which requires running CAQWs (N_p, α, θ_2) with no message, that can be achieved only by the modified QWHF-1. It is clear that for QHF [53], if the length of the bit string of the message is less than the number of nodes N, the system will be inefficient as some positions have zero probability.

7. Security analysis for the proposed authenticated protocols

7.1. The proposed AKD protocol

The main objective of an eavesdropper is to obtain fully/partly secret information from the data exchanged between the legitimate participants. Therefore, security analysis is an important evaluation criterion for any communication protocol. The security of the presented authenticated key distribution protocol is based on the physical properties of quantum walks and its key parameters. In this section, we present the security analysis of the proposed protocol in a detailed way and we show that the proposed AKD protocol is effective to detect any active attack.

7.1.1. Impersonation attack

In this kind of attack, Eve tries to play the role of Bob when communicating with Alice and on the other hand, she plays the role of Alice when transferring data to Bob, in order to get the fully shared secret key or at least a part of it. In the proposed protocol, we assume that Eve intends to play the role of Alice to communicate with Bob. In *Step 1* of the protocol, Eve publishes an integer odd number N_p with Bob to generate a bit string $B' \in \{0, 1\}^{8N_p^2}$ by running CAQWs (N, α, θ_2). However, it is very hard to generate the true hash value B, due to the fact that Eve does not possess the true key parameters (α, θ_2). Moreover, it is difficult for Eve to store the corresponding bit values of *ith*-bit of S when *ith*-bit of B is *"0"*. Eventually, Eve sends the bit sequence S to Bob and stores the bit string R according to its own bit string B'. In *Step 3* of the protocol, Bob stores R according to the correct

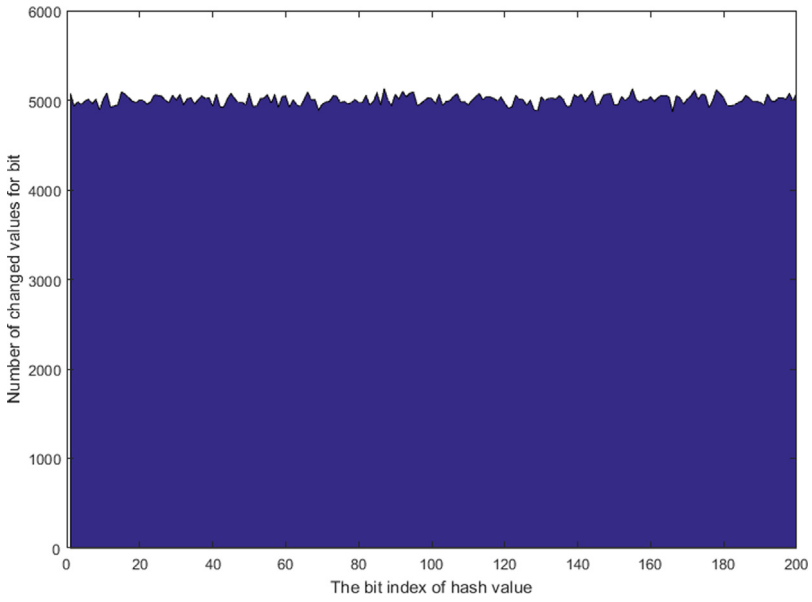


Fig. 11. The distribution of the hash value on hash space for QWHF-1.

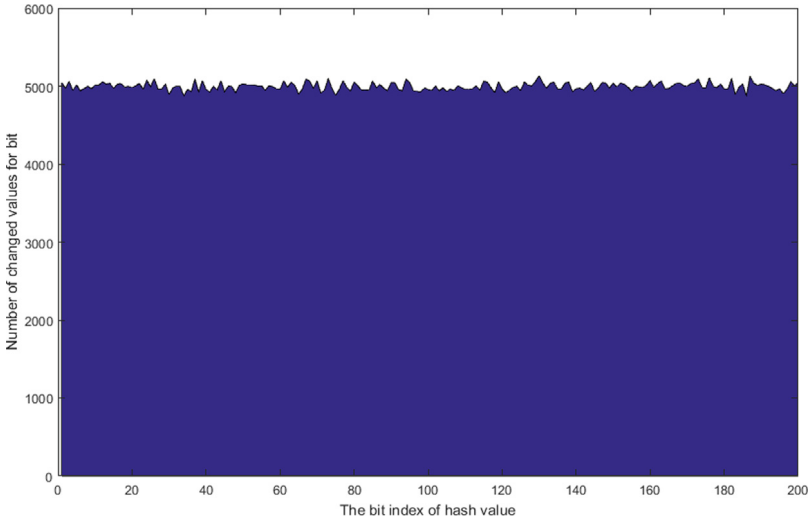


Fig. 12. The distribution of the hash value on hash space for QWHF-2.

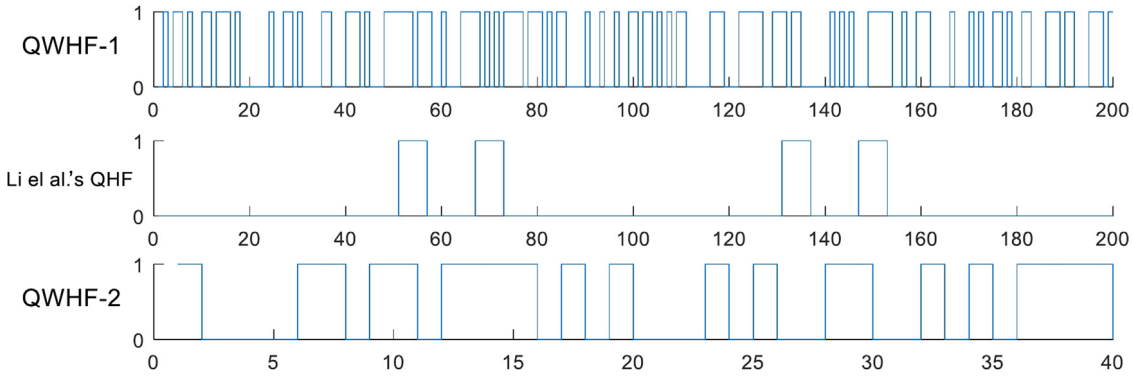


Fig. 13. 200-bit hash values for the message '*1*' and $N = 5$ for the three QHFs (QWHF-1, QHF [53], and QWHF-2) using the same parameters.

hash value B. Then Eve announces an integer odd number N_c to Bob in order to generate a checking bit string $K_c \in \{0, 1\}^{8N_c^2}$ by running CAQWs $(N_c, R, \alpha, \theta_0, \theta_1, \theta_2)$. The classical bit values R stored by Eve (*Step 2*) is different from that stored by Bob (*Step 3*) because the generated B sequence for both participants is different from each other as Eve does not possess the true key

parameters $\alpha, \theta_0, \theta_1, \theta_2$ (*Step 1*). Consequently, Bob detects the Eve's existence in *Step 5* of the protocol, once Eve announces the first $4 \times N_c^2$-bit of K_c, so the protocol terminated by Bob.

On the other hand, when Eve intends to impersonate Bob to deal with Alice, Eve would be detected by Alice in *Step 5* of the protocol, when Alice publishes the first $4 \times N_c^2$-bit of K_c sequence with Eve and waits for Eve to announce the remaining bits of K_c. By checking the announced bits with the remaining bits of K_c, Alice detects the existence of Eve and terminates the protocol. Moreover, Eve cannot deduce any information about the master key parameters $(\alpha, \theta_0, \theta_1, \theta_2)$, so the key parameters can be reused in the future.

7.1.2. Intercept–resend attack

In this kind of attack, Eve tries to deduce secret information by intercepting the sequence of bits S sent by Alice and then resends it to Bob.

In the proposed protocol, Eve tries to intercept the sequence of bits S sent by Alice. Eve does not possess any information about the key parameters (α, θ_2) to store the correct R according to the true hash value B. Eventually, Eve stores R randomly, then sends the sequence S to Bob. In *Step 3* of the protocol, Bob stores the *ith* bit of S when *ith* bit of B is *"0"* to obtain the classical bit string R. In *Step 5* of the protocol, Alice and Bob check K_c in order to detect Eve's existence as Eve sends the correct S as it was sent by Alice, so the protocol continues establishing the random secret key (*Step 6*). Eve may be successful to obtain R partly, however, she fails to deduce any information about the shared secret key as she does not possess the true master key parameters used to generate the secret key CAQWs $(N_k, R, \alpha, \theta_0, \theta_1, \theta_2)$. Therefore, the proposed authenticated key distribution protocol is secure against intercept–resend attack.

7.2. The proposed AQDC protocol

Security analysis is an essential evaluation criterion for any quantum protocol. In this section, we analyze several security aspects of our proposals.

7.2.1. Man-in-the-middle attack

Eve takes the role of Bob to communicate with Alice, and also acts as Alice to communicate with Bob in order to obtain the full secret message or a part of it. Eve is not able to know the parameters of the used QWHF-2 to send a fake sequence of photons to Bob. So, Bob will detect the existence of Eve and will abort the communication. Furthermore, if Eve impersonates Bob, Eve will not able to steal any information about the encoded secret message as she does not have any information about the used QHF. If Eve successfully measures the qubits with the correct basis, and gets the embedded hash code and the cipher text, she cannot deduce anything about the plain text because she does not have the full parameters for running the utilized QHF. So, our proposed quantum authentication protocol is secure against the man-in-the-middle attack.

7.2.2. Measurement attack

Eve aims at obtaining any information about the secret message by attacking the transferred qubits from Alice to Bob. Eve fails to deduce any part of the encoded secret message as she is not aware of the parameters used for QHF purposes. Any measurement performed by Eve on any qubit in the transferred sequence, will lead to different measurement results in the obtained bit sequence $B' = b'_1 b'_2 \dots b'_n b'_{n+1} b'_{n+2} \dots b'_{n+v}$ (cipher text + hash code). By checking the hash code v'_1 obtained from the bit sequence B' with the hash value v_4 for the recovered message, Bob can detect any measurement on the transmitted qubits. So, the measurement attack has no effect on the presented quantum authentication protocol.

7.2.3. Message attack

When Alice sends the sequence of photons to Bob, Eve can receive it, however, she cannot infer any information about the secret message, because she does not have any information about the used QWHF-2. In the unlikely event that she succeeded in measuring the qubits and obtained the embedded hash code and the cipher text, she would not be able to deduce any information about the plain text because she would not know the parameters used for QHF. So, our proposed protocol is secure against message attack.

7.2.4. No-message attack

Assume that an eavesdropper, Eve generates a sequence of photons and sends it to Bob. The goal of Eve is to make Bob believe that the embedded secret message in this sequence originates from Alice. When Bob receives the sequence, he cannot be sure whether it comes from Alice or from an eavesdropper. Then Bob extracts the hash code v'_1 and b' from B' and gets the hash value v_3 for v'_1. Next, he executes the XOR operation to the bit sequence b' and the hash value v_3 to obtain the bit string m′. Then he converts it to the string message and in result gets the hash value v_4 for the recovered message and verifies it with the hash code v'_1. So, Bob detects the existence of Eve and aborts the protocol.

8. Concluding remarks

The main feature of 5G networks is that they will play a central role in our daily life. Moreover, as they utilize many promising communication technologies and will support a huge number of connected devices this will surely bring tremendous challenges for the trust, security and privacy. Therefore, secure mechanisms and protocols are required as the basis for 5G networks to address this problem and follow security-by-design but also security-by-operations rules. Inspired by the limitations of the classical cryptosystems and the advantages of quantum walks, in this paper we proposed new constructions of cryptosystems to achieve secure information sharing and data protection which are based on quantum technologies. First, we proposed two efficient hash function mechanisms for 5G applications based on QWs, namely QWHF-1 and QWHF-2. Then, based on the two hash function proposals, two efficient security protocols for securing the data in 5G networks scenario have been introduced. Conducted performance analyses and simulation results proved that the proposed approaches are characterized with high security, efficiency, and robustness against several well-known attacks which make them suitable for utilization within various 5G applications.

Acknowledgments

Ahmed A. Abd EL-Latif gratefully acknowledges the financial support of Faculty of Science, Menoufia University, Egypt. Salvador E. Venegas-Andraca gratefully acknowledges the financial support of Tecnologico de Monterrey, Escuela de Ingenieria y Ciencias and CONACyT, Mexico (SNI number 41594 as well as Fronteras de la Ciencia project No. 1007).

Moreover, this research was partially funded by the National Centre for Research and Development, Poland under Gospostrateg Programme framework, and more specifically 5G@PL project entitled "Deployment of 5G network in Polish market" grant agreement : Gospostrateg 1/383021/19/NCBR/2018.

The authors warmly thank their families for their unconditional support.

Conflict of interest

None.

Declaration of competing interest

The authors declared that they had no conflicts of interest with respect to their authorship or the publication of this article.

References

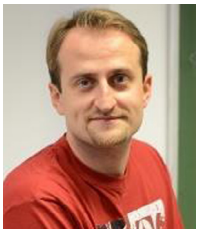
[1] S. Li, L. Da Xu, S. Zhao, 5g internet of things: A survey, J. Ind. Inf. Integr. 10 (2018) 1–9.
[2] K. Fan, Y. Gong, C. Liang, H. Li, Y. Yang, Lightweight and ultralightweight rfid mutual authentication protocol with cache in the reader for iot in 5g, Secur. Commun. Netw. 9 (16) (2016) 3095–3104.
[3] J. Ni, X. Lin, X.S. Shen, Efficient and secure service-oriented authentication supporting network slicing for 5g-enabled iot, IEEE J. Sel. Areas Commun. 36 (3) (2018) 644–657.
[4] Q. Wang, D. Chen, N. Zhang, Z. Qin, Z. Qin, Lacs: A lightweight label-based access control scheme in iot-based 5g caching context, IEEE Access 5 (2017) 4018–4027.
[5] K. Fan, Y. Gong, Z. Du, H. Li, Y. Yang, Rfid secure application revocation for iot in 5g, in: 2015 IEEE Trustcom/BigDataSE/ISPA, vol. 1, IEEE, 2015, pp. 175–181.
[6] M.R. Palattella, M. Dohler, A. Grieco, G. Rizzo, J. Torsner, T. Engel, L. Ladid, Internet of things in the 5g era: Enablers, architecture, and business models, IEEE J. Sel. Areas Commun. 34 (3) (2016) 510–527.
[7] K. Fan, P. Song, Y. Yang, Ulmap: Ultralightweight nfc mutual authentication protocol with pseudonyms in the tag for iot in 5g, Mob. Inf. Syst. (2017).
[8] F. Al-Turjman, 5g-enabled devices and smart-spaces in social-iot: an overview, Future Gener. Comput. Syst. 92 (2019) 732–744.
[9] N.-N. Dao, M. Park, J. Kim, J. Paek, S. Cho, Resource-aware relay selection for inter-cell interference avoidance in 5g heterogeneous network for internet of things systems, Future Gener. Comput. Syst. 93 (2019) 877–887.
[10] S.H. Ahmed, S. Rani, A.hybrid. approach, A hybrid approach smart street use case and future aspects for internet of things in smart cities, Future Gener. Comput. Syst. 79 (2018) 941–951.
[11] O. Bello, S. Zeadally, Toward efficient smartification of the internet of things (iot) services, Future Gener. Comput. Syst. 92 (2019) 663–673.
[12] L. Nkenyereye, C.H. Liu, J. Song, Towards secure and privacy preserving collision avoidance system in 5g fog based internet of vehicles, Future Gener. Comput. Syst. 95 (2019) 488–499.
[13] X. Zhang, A. Kunz, S. Schröder, Overview of 5g security in 3gpp, in: 2017 IEEE Conference on Standards for Communications and Networking (CSCN), IEEE, 2017, pp. 181–186.
[14] D. Fang, Y. Qian, R.Q. Hu, Security for 5g mobile wireless networks, IEEE Access 6 (2018) 4850–4874.
[15] M.A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, H. Janicke, Security for 4g and 5g cellular networks: A survey of existing authentication and privacy-preserving schemes, J. Netw. Comput. Appl. 101 (2018) 55–82.
[16] B. Song, Y. Cheong, T. Lee, J. Jeong, Design and security analysis of improved identity management protocol for 5g/iot networks, in: World Conference on Information Systems and Technologies, 2017, pp. 311–320.
[17] R. Giustolisi, C. Gerhmann, Threats to 5g group-based authentication, in: 13th International Conference on Security and Cryptography, SECRYPT, SciTePress, Madrid, Spain, 2016, pp. 26–28.
[18] E. Dubrova, M. Naslund, G. Selander, Crc-based message authentication for 5g mobile technology, In 2015, 2015, pp. 1186–1191.
[19] I. Butun, M. Erol-Kantarci, B. Kantarci, H. Song, Cloud-centric multi-level authentication as a service for secure public safety device networks, IEEE Commun. Mag. 54 (4) (2016) 47–53.
[20] M.H. Au, K. Liang, J.K. Liu, R. Lu, J. Ning, Privacy-preserving personal data operation on mobile cloud-hances and challenges over advanced persistent threat, Future Gener. Comput. Syst. 79 (2018) 337–349.
[21] R. Roman, J. Lopez, M. Mambo, Mobile.edge. computing, fog, et al., Mobile edge computing fog others : A survey and analysis of security threats and challenges, Future Gener. Comput. Syst. 78 (2018) 680–698.
[22] B. Varghese, R. Buyya, Next generation cloud computing: New trends and research directions, Future Gener. Comput. Syst. 79 (2018) 849–861.
[23] S. Yang, D. Yin, X. Song, X. Dong, G. Manogaran, G. Mastorakis, C.X. Mavromoustakis, J.M. Batalla, Security situation assessment for massive mimo systems for 5g communications, Future Gener. Comput. Syst. 98 (2019) 25–34.
[24] R.P. Jover, Some key challenges in securing 5g wireless networks, Electr. Comment Filing Syst. (Jan) (2017).
[25] D. Schinianakis, Alternative security options in the 5g and iot era, IEEE Circuits Syst. Mag. 17 (4) (2017) 6–28.
[26] R. Chaudhary, N. Kumar, S. Zeadally, Network service chaining in fog and cloud computing for the 5g environment: Data management and security challenges, IEEE Commun. Mag. 55 (11) (2017) 114–122.
[27] Z. Yan, H. Xie, P. Zhang, B.B. Gupta, Flexible data access control in d2d communications, Future Gener. Comput. Syst. 82 (2018) 738–751.
[28] S. Bakhtiari, R. Safavi-Naini, J. Pieprzyk, Cryptographic Hash Functions: A Survey, Centre for Computer Security Research, Department of Computer Science, University of Wollongong, Australie, 1995.
[29] J.L. Carter, M.N. Wegman, Universal classes of hash functions, J. Comput. Syst. Sci. 18 (2) (1979) 143–154.
[30] M. Amin, O.S. Faragallah, A.A.A. El-Latif, Chaos-based hash function (cbhf) for cryptographic applications, Chaos Solitons Fractals 42 (2) (2009) 767–772.
[31] X. Wang, H. Yu, How to break md5 and other hash functions, in: R. Cramer (Ed.), Advances in Cryptology – EUROCRYPT 2005, Springer Berlin Heidelberg, Berlin, Heidelberg, 2005, pp. 19–35.
[32] X. Wang, X. Lai, D. Feng, H. Chen, X. Yu, Cryptanalysis of the hash functions md4 and ripemd, in: R. Cramer (Ed.), Advances in Cryptology – EUROCRYPT 2005, Springer Berlin Heidelberg, Berlin, Heidelberg, 2005, pp. 1–18.
[33] A. Buhari, Z.A. Zukarnain, S.K. Subramaniam, H. Zainuddin, S. Saharudin, A quantum based challenge-response user authentication scheme over noiseless channel, Int. J. Netw. Secur. Appl. 4 (2012) 67.
[34] T. Tsurumaru, M. Hayashi, Dual universality of hash functions and its applications to quantum cryptography, IEEE Trans. Inform. Theory 59 (7) (2013) 4700–4717.
[35] T. Hwang, Y.P. Luo, C.W. Yang, T.H. Lin, Quantum authencryption: one-step authenticated quantum secure direct communications for off-line communicants, Quantum Inf. Process. 13 (4) (2014) 925–933.
[36] X. Xin, X. Hua, J. Song, F. Li, Quantum authentication protocol for classical messages based on bell states and hash function, Int. J. Secur. Appl. 9 (7) (2015) 285–292.
[37] A.A.A. El-Latif, B. Abd-El-Atty, M.S. Hossain, S. Elmougy, A. Ghoneim, Secure quantum steganography protocol for fog cloud internet of things, IEEE Access 6 (2018) 10332–10340.
[38] X. Xin, X. Hua, C. Li, D. Chen, Quantum authentication of classical messages using non-orthogonal qubits and hash function, Int. J. u-and e-Service Sci. Technol. 9 (10) (2016) 181–186.
[39] B. Ying, A. Nayak, Lightweight remote user authentication protocol for multi-server 5g networks using self-certified public key cryptography, J. Netw. Comput. Appl. (2019).
[40] L.A. Amaral, E. de Matos, R.T. Tiburski, F. Hessel, W.T. Lunardi, S. Marczak, Middleware Technology for Iot Systems: Challenges and Perspectives Toward 5g, 2016.
[41] S. Shin, T. Kwon, Two-factor authenticated key agreement supporting unlinkability in 5g-integrated wireless sensor networks, IEEE Access 6 (2018) 11229–11241.
[42] E.-M. Oproiu, M. Iordache, C. Patachia, C. Costea, I. Marghescu, Development and implementation of a smart city use case in a 5g mobile network's operator, in: 2017 25th Telecommunication Forum, TELFOR, IEEE, 2017, pp. 1–4.
[43] A. Sk, V. Masilamani, A novel digital watermarking scheme for data authentication and copyright protection in 5g networks, Comput. Electric. Eng. 72 (2018) 589–605.
[44] X. Li, F. Wu, M.K. Khan, L. Xu, J. Shen, M. Jo, A secure chaotic map-based remote authentication scheme for telecare medicine information systems, Future Gener. Comput. Syst. 84 (2018) 149–159.
[45] A. Irshad, M. Sher, H.F. Ahmad, B.A. Alzahrani, S.A. Chaudhry, R. Kumar, An improved multi-server authentication scheme for distributed mobile cloud computing services, TIIS 10 (12) (2016) 5529–5552.
[46] M.A. Jan, F. Khan, M. Alam, M. Usman, A payload-based mutual authentication scheme for internet of things, Future Gener. Comput. Syst. 92 (2019) 1028–1039.
[47] C. Guo, N. Luo, M.Z.A. Bhuiyan, Y. Jie, Y. Chen, B. Feng, M. Alam, Key-aggregate authentication cryptosystem for data sharing in dynamic cloud storage, Future Gener. Comput. Syst. 84 (2018) 190–199.
[48] E.O. Kiktenko, N.O. Pozhar, M.N. Anufriev, A.S. Trushechkin, R.R. Yunusov, Y.V. Kurochkin, A.I. Lvovsky, A.K. Fedorov, Quantum-secured blockchain, Quantum Sci. Technol. 3 (3) (2018) 035004.
[49] A.A.A. E.L.-L.atif, B. Abd-El-Atty, S.E. Venegas-Andraca, A novel image steganography technique based on quantum substitution boxes, Opt. Laser Technol. 116 (2019) 92–102.
[50] D. Li, J. Zhang, F.Z. Guo, W. Huang, Q.Y. Wen, H. Chen, Discrete-time interacting quantum walks and quantum hash schemes, Quantum Inf. Process. 12 (3) (2013) 1501–1513.
[51] C. Vlachou, J. Rodrigues, P. Mateus, N. Paunković, A. Souto, Quantum walks public key cryptographic system, Int. J. Quantum Inf. 13 (7) (2015) 1550050.
[52] Y.G. Yang, P. Xu, R. Yang, Y.H. Zhou, W.M. Shi, Quantum hash function and its application to privacy amplification in quantum key distribution, pseudo-random number generation and image encryption, Sci. Rep. 6 (2016) 19788.

[53] D. Li, Y.G. Yang, J.L. Bi, J.B. Yuan, J. Xu, Controlled alternate quantum walks based quantum hash function, Sci. Rep. 8 (2018) 225.
[54] Y.G. Yang, J.L. Bi, X.B. Chen, Z. Yuan, Y.H. Zhou, W.M. Shi, Simple hash function using discrete-time quantum walks, Quantum Inf. Process. 17 (8) (2018) 189.
[55] W.F. Cao, Y.C. Zhang, Y.G. Yang, D. Li, Y.H. Zhou, W.M. Shi, Constructing quantum hash functions based on quantum walks on johnson graphs, Quantum Inf. Process. 17 (7) (2018) 156.
[56] S.E. Venegas-Andraca, Quantum walks: a comprehensive review, Quantum Inf. Process. 11 (5) (2012) 1015–1106.
[57] H. Luo, P. Xue, Properties of long quantum walks in one and two dimensions, Quantum Inf. Process. 14 (12) (2015) 4361–4394.
[58] N. Konno, H. Mitsuhashi, I. Sato, The discrete-time quaternionic quantum walk on a graph, Quantum Inf. Process. 15 (2) (2016) 651–673.
[59] Y.G. Yang, Q.X. Pan, S.J. Sun, P. Xu, Novel image encryption based on quantum walks, Sci. Rep. 5 (2015) 7784.
[60] A. Bhosle, Improving performance and securing data in manet with aes, Int. J. Res. Advent Technol. 1.
[61] B. Abd-El-Atty, S.E. Venegas-Andraca, A.A.A. El-Latif, Quantum information protocols for cryptography, in: Quantum Computing: An Environment for Intelligent Large Scale Real Application, 2018, pp. 3–23.
[62] Y.P. Luo, T. Hwang, Authenticated semi-quantum direct communication protocols using bell states, Quantum Inf. Process. 15 (2) (2016) 947–958.
[63] S. Almousa, M. Barbeau, Delay and reflection attacks in authenticated semi-quantum direct communications, in: 2016 IEEE Globecom Workshops, GC Wkshps, IEEE, 2016, pp. 1–7.

Ahmed A. Abd El-Latif received the B.Sc. degree with honor rank in Mathematics and Computer Science in 2005 and M.Sc. degree in Computer Science in 2010, all from Menoufia University, Egypt. He received his Ph.D. degree in Computer Science & Technology at Harbin Institute of Technology (H.I.T), Harbin, P. R. China in 2013. He is an associate professor of Computer Science at Menoufia University, Egypt and School of Information Technology and Computer Science, Nile University, Egypt. He is author and co-author of more than 100 papers, including refereed IEEE/ACM/Springer/Elsevier journals, conference papers, and book chapters. He is a referee of many referred international repute journals and conferences. He received many awards, State Encouragement Award in Engineering Sciences 2016, Arab Republic of Egypt; the best Ph.D. student award from Harbin Institute of Technology, China 2013; Young scientific award, Menoufia University, Egypt 2014. He is a fellow at Academy of Scientific Research and Technology, Egypt. His areas of interests are multimedia content encryption, secure wireless communication, IoT, applied cryptanalysis, perceptual cryptography, secret media sharing, information hiding, biometrics, forensic analysis in digital images, and quantum information processing.

Bassem Abd-El-Atty received B.S. degree in physics and computer science, and M.Sc. degree in computer science from Menoufia University, Egypt, in 2010 and 2017, respectively. He is currently pursuing the PhD degree in quantum information processing at the school of Mathematics and computer science, Faculty of Science, Menoufia University, Egypt. His research interests include quantum information processing and image processing.

Salvador E. Venegas-Andraca is a Professor of Computer Science and head of the Quantum Information Processing group at Tecnologico de Monterrey. He holds a DPhil in Physics awarded by the University of Oxford, he is a leading scientist in the field of quantum walks, cofounder of the field Quantum Image Processing and his research interests include quantum algorithms as well as the algorithmic analysis of NP-hard/NP-complete problems. Professor Venegas-Andraca has published over 40 scientific papers and is the author of Quantum Walks for Computer Scientists (2008), the first book ever written on the scientific field of quantum walks. He is a fellow of the Mexican Academy of Sciences and senior member of the Association for Computing Machinery.



Wojciech Mazurczyk received the B.Sc., M.Sc., Ph.D. (Hons.), and D.Sc. (habilitation) degrees in telecommunications from the Warsaw University of Technology (WUT), Warsaw, Poland, in 2003, 2004, 2009, and 2014, respectively. He is currently an Associate Professor with the Institute of Telecommunications, WUT, where he is the Head of the Bio-Inspired Security Research Group (bsrg.tele.pw.edu.pl). He is also a Researcher at the Parallelism and VLSI Group at Faculty of Mathematics and Computer Science at FernUniversitaet, Germany. His research interests include bioinspired cybersecurity and networking, information hiding, and network security. He is involved in the technical program committee of many international conferences and also serves as a reviewer for major international magazines and journals. From 2016 he is Editor-in-Chief of an open access Journal of Cyber Security and Mobility, and from 2018 he is serving as an Associate Editor of the IEEE Transactions on Information Forensics and Security and as Mobile Communications and Networks Series Editor for the IEEE Communications Magazine. He is also a Senior Member of IEEE.