Journal of information and communication convergence engineering
http://jicce.org

J. Inf. Commun. Converg. Eng. 20(4): 242-249, Dec. 2022 Regular paper

Quantum Computing Cryptography and Lattice Mechanism

Abbas M. Ali Al-muqarm[1], Firas Abedi[2], and Ali S. Abosinnee[3]*

[1]Computer Technical Engineering Department, The Islamic University, Najaf 54001, Iraq
[2]Al-Zahraa University for Women, Karbala 56001, Iraq
[3]Altoosi University College, Najaf 54001, Iraq

Abstract

Classical cryptography with complex computations has recently been utilized in the latest computing systems to create secret keys. However, systems can be breached by fast-measuring methods of the secret key; this approach does not offer adequate protection when depending on the computational complexity alone. The laws of physics for communication purposes are used in quantum computing, enabling new computing concepts to be introduced, particularly in cryptography and key distribution. This paper proposes a quantum computing lattice (CQL) mechanism that applies the BB84 protocol to generate a quantum key. The generated key and a one-time pad encryption method are used to encrypt the message. Then Babai's algorithm is applied to the ciphertext to find the closet vector problem within the lattice. As a result, quantum computing concepts are used with classical encryption methods to find the closet vector problem in a lattice, providing strength encryption to generate the key. The proposed approach is demonstrated a high calculation speed when using quantum computing.

Index Terms: Quantum Cryptography, Key Distribution, BB84 Protocol, Lattice, CVP

I. INTRODUCTION

Human civilization has entered the information era owing to the widespread use and rapid growth of the Internet. Almost all aspects in life are now inextricably linked to the Internet [1]. In our modern times, secure communication has been widely used and is an important approach; however, we must remember that important information is often sent over a network. With an increased number of email and Internet users, it would be easy for hackers to eavesdrop. Despite encrypting information using cryptographic schemes, because the protection of a cryptogram depends on the confidentiality of the key applied, a vulnerability remains (secret key encryption and public-key cryptography). To prevent this key from being revealed and to avoid the issue of a key distribution, two users must meet in advance to settle on the key or use private information with secret key cryptography (SKC) or large numbers and a difficult processing, all of which are inconvenient approaches [2]. Owing to the disadvantages of basic cryptographic systems, quantum cryptography must be used to make the transmission of information between two or more parties safer. To solve this problem, the strength and privacy are contained within the laws of physics. The peculiar and irregular behaviors of microscopic (photons) enables users to create secret keys and securely detect eavesdropping. The distribution of quantum keys is the subject of quantum cryptography. Quantum cryptography is the technique and science for using the effect of quantum mechanics to carry out cryptographic tasks. It offers a perfectly secure data transmission because it relies on the laws of physics [3]. Quantum cryptography is a subfield of cryptography that combines quantum mechanics with traditional

Received 22 February 2022, **Revised** 14 October 2022, **Accepted** 18 October 2022
***Corresponding Author** Ali S. Abosinnee (E-mail: abosinnee.ali@gmail.com, Tel: +964-7735090633)
Altoosi University College, Najaf 54001, Iraq

Open Access https://doi.org/10.56977/jicce.2022.20.4.242 print ISSN: 2234-8255 online ISSN: 2234-8883

cryptography. Heisenberg's uncertainty principle and quantum no-cloning theory may ensure communication security [4]. Many existing public-key encryption (e.g., ElGamal, RSA, elliptic curve cryptography (ECC)) approaches are insecure in a quantum computer owing to its particular features. Under quantum computers, the well-known discrete logarithm problem (DLP) or the integer factorization problem will no longer be complex [5].

The rest of this paper is organized as follows. Section 2 introduces some related studies regarding quantum cryptography. Section 3 presents the preliminaries of quantum physics and quantum communication. Section 4 presents the benefits and security that quantum cryptography will bring to the future Internet. Section 5 provides some concluding remarks regarding this paper.

II. RELATED WORK

One of the quantum cryptography protocols is the quantum authentication (QA) protocol, which was suggested in 2001. Many QA protocols have since been proposed [6,7,8]. In 2011, Bennett and Brassard presented the first practical quantum key distribution (QKD) protocol. They were the first to establish the quantum key distribution mechanism by utilizing single-photon polarization. Then, to increase the security and efficiency, significant effort was placed into the development of QKD [9]. According to Sudhir et al. (2017), the Internet of Things (IoT) will play a significant role in our lives during the next several years. The current level of protection for future IoT apps is poor. Quantum cryptography as a long-term security solution for IoT has been introduced [10]. Balygin et al. (2020) developed a detector mismatch attack, which involves only minimal changes to the current systems that use the BB84 quantum distribution protocol, which implies a simple and physically intuitive concept of defense against an active sensing attack [11]. Krendelev and Sazonova (2018) described an algorithm for creating a hash function, which is resistant to quantum computers, based on the problem of a system for solving polynomial equations with integers. The developed algorithm is parameterized such that the result of the hash function depends on several parameters, and it will therefore take considerably longer to select the solution to the task because finding a solution to the described system of equations with a degree of greater than 3 is algorithmically unsolvable [12]. This paper introduces some useful quantum computing techniques for AI engineers, including quadratic unconstrained binary optimization (QUBO), variational quantum Eigensolver (VQE), the quantum approximate optimization algorithm (QAOA), and the Harrow-Hassidim-Lloyd (HHL) algorithm [13].

III. QUANTUM CRYPTOGRAPHY AND PROTOCOLS

Quantum cryptography cannot be used to exchange information securely; however, two users can use it to share a cryptographic key. For this reason, we generally refer to a quantum key distribution as quantum cryptography. Bennett and Brassard invented QKD in 1984, which can enable us to securely solve the distribution issue of a random key.

In quantum computers, the qubit is the smallest piece of a memory system unit and is identical to a bit in classical computers. In classical computers, the bit is the most significant element, and the value stored as a bit is either a 0 or 1.

The bit is the most significant element in classical computers; however, in quantum mechanics, the unit is the qubit, which has a minimum of two values. A qubit is represented as a 0 or 1 between "|" and ">," and thus is represented as | 0> and | 1>, as shown in Fig. 1 [14].

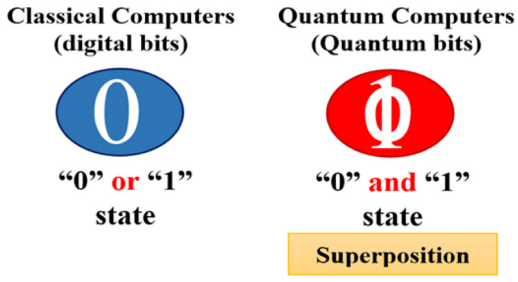

Fig. 1. Classical and quantum bits

In a mathematics representation, the qubits are represented as a vector of the column, where the binary state of "0" represents a vector of a column of [1,0], whereas the binary state of "1" is a column of a vector of [0,1]; however, it is possible to portray them better using a Dirac notation in mathematics, which is also called a "bra-ket notation." In a Dirac notation, the qubit of a 0 state is represented as |0>, whereas the qubit of a 1 state is |1>.

The rectilinear basis (+) of the horizontal (0^o) and vertical (90^o) polarization states, where |→> and |↑> denote (0^o) and (90^o) polarized photons, respectively, and the vector space (Jones Matrix) for both states are shown in Fig. 2.

The diagonal basis (X) of the diagonal polarization states are 45^o and 135^o, where |↗> and |↖> denote photons polarized at 45^o and 135^o, respectively. The expressions for the vector space of both states are indicated in Equations (1) and (2), and Fig. 3 shows the different states of the photons [11].

$$|0>=\begin{bmatrix}1\\0\end{bmatrix}$$

$$|1>=\begin{bmatrix}0\\1\end{bmatrix}$$

Fig. 2. Vector space (Jones Matrix) horizontally and vertically

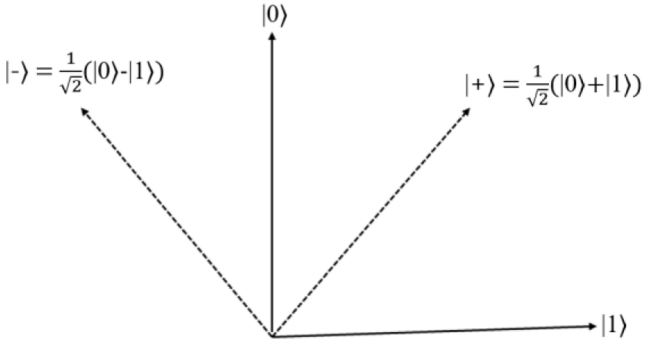

Fig. 3. Different states of photons

$$|\nearrow>=\begin{vmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{vmatrix}=\frac{1}{\sqrt{2}}\begin{vmatrix}1\\0\end{vmatrix}+\frac{1}{\sqrt{2}}\begin{vmatrix}0\\1\end{vmatrix}=\frac{1}{\sqrt{2}}\begin{vmatrix}\rightarrow>+\frac{1}{\sqrt{2}}|\uparrow> \quad (1)$$

$$|\nwarrow>=\begin{vmatrix}\frac{1}{\sqrt{2}}\\ -\frac{1}{\sqrt{2}}\end{vmatrix}=\frac{1}{\sqrt{2}}\begin{vmatrix}1\\0\end{vmatrix}-\frac{1}{\sqrt{2}}\begin{vmatrix}0\\1\end{vmatrix}=\frac{1}{\sqrt{2}}\begin{vmatrix}\rightarrow>-\frac{1}{\sqrt{2}}|\uparrow> \quad (2)$$

Figure 4 (a and b) shows the Classical bits agents Qubits

$$0 \rightarrow |0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$$

$$1 \rightarrow |1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$$

(a)

$$|\Psi\rangle = \begin{pmatrix}\alpha\\\beta\end{pmatrix} = \underline{\alpha|0\rangle} + \underline{\beta|1\rangle}$$

(b)

Fig. 4. (a) Classical bits (b) Qubits

The superposition of |0> and |1> has the same length as the real vectors, as indicated in Equation (3) and Fig. 5.

$$\alpha 2 + \beta 2 = 1 \quad (3)$$

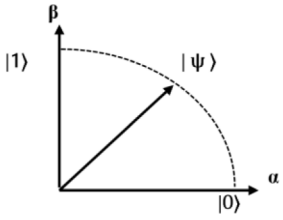

Fig. 5. Superposition of |0) and (1) having the same length for real vectors

A. Protocol E91

Arthur developed the E91 protocol in 1991. Entangled photons are used in this protocol. Alice, Bob, or any third party should therefore prepare for such application. Figure 6 illustrates the described bases on a Poincare sphere. Measuring from the positive x-axis, one can see that Alice's bases are lined up at angles of 0°, 45°, and 90°, whereas Bob's bases are located at 45°, 90°, and 135° [2].

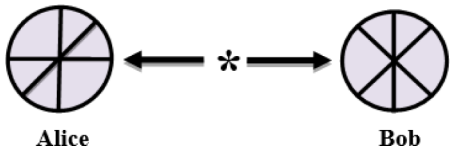

Fig. 6. Illustration of the described bases on a Poincare sphere

This protocol is dependent on the following steps, as illustrated in Fig. 7.

Algorithm of Protocol E91:
Input: Source generates entangled particles
Output: Get common key
Step 1: Begin {
Step 2: Source generates entangled particles.
Step 3: Send particles to Alice and Bob.
Step 4: Measure particles independently.
Step 5: Send schemes from one party to another.
Step 6: Compare schemes and get common key.
Step 7: Send hashes to each other to verify the equality of the common key.
Step 8: } End Algorithm

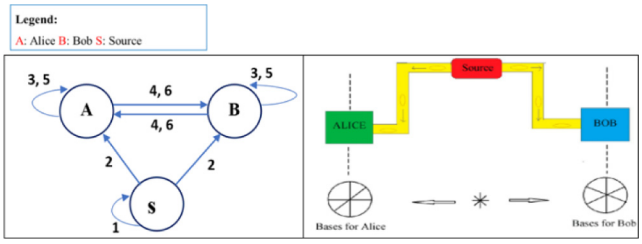

Fig. 7. Protocol E91 Mechanism

B. BB84 Protocol

BB84 and the DARPA project use photon polarization to encrypt the data bits, relying on "uncertainty" to prevent Eve from discovering the hidden key. In 1984, the first quantum cryptography protocol was implemented by Bennet and Brassard. They start from the study "Conjugate Coding" by Wiesner and then use photon polarization for the key distribution. The polarization states represent both orthogonal bases for linear polarization (+) and diagonal bases for diag-

onal polarization (×). Figure 8 shows the rectilinear and diagonal bases [15].

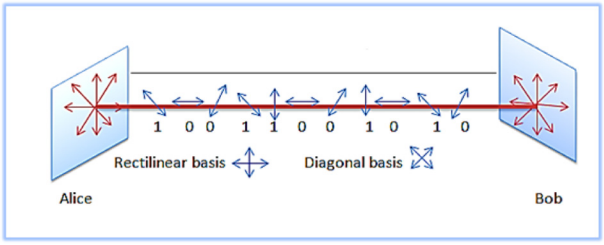

Fig. 8. Rectilinear and diagonal bases

The following notations are used: (I) denotes a photon in a horizontally polarized state or at 0° degrees, (–) denotes a photon inside a vertically polarized state or at 90°, (/) denotes a photon in a 45° degree polarization, and (\) denotes a photon in a 135° degree polarization. The 0° and 45° degrees are measured as bit "0," and 90° and 135° are measured as bit "1," as shown in Table 1.

Table 1. Notation of bases and polarization

Bases	Polarization	Bit	Polarization angle
+	I	0	0°
+	-	1	90°
×	/	0	45°
×	\	1	135°

Two participants, Bob and Alice, would like to negotiate on an agreement of a secret key for this protocol, from which no eavesdropper, usually called Eve, can access essential data. Alice produces a random sequence of bits, sending it through a quantum channel to Bob in various polarization bases (measured as bits). When Bob receives the sequence, also called a "raw key," Bob chooses the basis of each qubit. His examination is either similar to or different than Alice's basis. Bob announces his bases through a public channel, and only a bit that is similar to Alice's bases will then be used as a secret key, with the rest discarded. A non-similar bit or a short bit that Bob hasn't measured is referred to as a "sifted key" [15].

The algorithm and steps applied by the BB84 protocol are as follows [16]:

Algorithm of BB84 protocol:
Input: Random bit
Output: Shared secret key
Step 1: Begin {
Step 2: Alice's random bit.
Step 3: Alice's random sending basis.
Step 4: Photon polarization sent by Alice.
Step 5: Bob's random measurement basis.
Step 6: Photon polarization measured by Bob.
Step 7: Public discussion of basis.
Step 8: Shared secret key.
Step 9:} End algorithm.

Example applying the above algorithm:

1: Let us take the sequence (1001110010) randomly chosen by Alice to generate a key used for any following encryption method.

2: Alice will randomly pick the polarization and then give it to Bob.

3: The polarization is estimated by Bob and compared with Alice to see the correct polarization.

4: Bob will convert the correct polarization into a series of 1s and 0s.

5: This series represents the key.

IV. ERROR ESTIMATION

The quantum bit error rate (QBER) is the quantum cryptography error rate method used and is defined as the percentage of error that occurs in the key during transmission. If the quantum cryptography of BB84 is properly constructed, the existence of an eavesdropper would be easy to discover. The eavesdropper obtains further data with a greater error rate, as shown in Equation (4) [14,15].

$$QBER = N_{wrong}/(Ls+N_{wrong}), \quad (4)$$

where Ls is the number of bits from a primary sequence, and N_{wrong} indicates the number of bit errors.

Example of Error Estimation

Alice generates a sequence from primary bits with a length of 750 (Ls = 750) and a bit error (number of wrong bits that occurred between Alice and Bob) sequence with a length of N_wrong = 320.

Thus, QBER = 320/(750 + 320) = 0.29.

A value (0.29) of less than 50% means that there is no eavesdropper and the right bits can be used as a secret shared key.

V. QUANTUM CRYPTOGRAPHY ADVANTAGES AND DISADVANTAGES

A quantum cryptosystem demonstrates certain advantages over symmetric and other public-key crypto algorithms. The application of quantum cryptography is a big part of digital communication in our everyday lives [17,18,19].

1) The advantages are as follows:
   a) Easy to use.
   b) Almost unbreakable
   c) Requires the fewest resources.
2) The disadvantages are as follows:
   The quantum signal range is currently limited to approximately 90 miles.
3) Applications include the following:
   a) Data encryption.
   b) Digital signature.
   c) Communication security within a space.
   d) Quantum Internet.
   e) Brain analysis functionality.

VI. "ONE-TIME PAD" ENCRYPTION

The “one-time pad” (OTP) used in cryptography is a method of encryption that cannot be cracked; however, this requires using one pre-shared key of the selfsame size, or a key longer than the message that we need to send. With this method, the plaintext can be encrypted using the random key (a one-time pad is often referenced). Then, every character bit in the plaintext is encrypted by combining it with the right bit or character from the pad. If the following four conditions are satisfied, it will be challenging to crack the resulting ciphertext:

The key should be genuinely random.
The key must be at least as lengthy as the plaintext.
The key should be not entirely or partially re-used.
It is vital to keep the key entirely secretive.
The encryption equation of a one-time pad is as follows:

$$c1 = pl \oplus k \tag{5}$$

VII. LATTICE AND CLOSEST VECTOR PROBLEM

The problem of the closest vector (CVP) is to give vector ($w \in R$) which is not contained in the lattice (L), and then find vector $v \in L$ that is close to vector w, e.g., find a vector ($v \in L$), which lessens the Euclidean norm, as in ($w - v$). Suppose that we want to find a vector that is contended in (L). In addition, it is close to vector w, $\in R\hat{}n$ based on Babai’s algorithm:

Babai’s Closest Algorithm:
Write w = t1v1 + t2v2 + · · · + tnvn with t1, . . . , tn∈R.
Set ai = _ti! for i = 1, 2, . . . , n.
Return the vector v = a1v1 + a2v2 + · · · + anvn.a

VIII. PROPOSED METHOD

This section introduces the proposed method, called quantum computing and lattices (CQL). In our proposed approach, we generate a quantum key (shared secret key) depending on the BB84 protocol, and thus we use a key generated to encrypt a message through the OTP method, as in Equation (5). In cryptography, a one-time pad is a system in which a private key is randomly generated. We then use the ciphertext to create a lattice, and thus we apply Babai’s algorithm to find the closest vector. As shown in Fig. 9, the proposed algorithm and schemes are implemented in MATLAB.

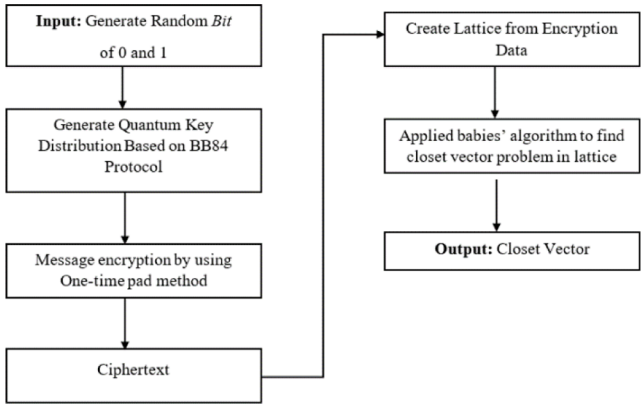

Fig. 9. Proposed CQL scheme

Proposed Algorithm:
Input: Random bit as a binary 0 or 1
Output: Closet vector
Step 1: Begin {
Step 2: Generate a quantum key distribution based on the BB84 protocol
Step 3: Use one-time pad encryption as in Equation (5) to encrypt a message with a key from Step 2
Step 4: Create a lattice from the encryption data
Step 5: Apply Babais’ algorithm to find the closet vector problem in a lattice
Step 6:} End algorithm.

The proposed system starts from generating bits (0s or 1s), into a ciphertext and then creating a lattice from the ciphertext. Babai’s algorithm used to find the CVP in this system can then be easily used with any encryption teaching. The reason for this is the strength of the key generated using the quantum protocol.

IX. IMPLEMENTATION AND RESULTS OF CQL

In this section, implementation the proposed algorithm using MATLAB R2019b is described. Random bits of 0s and 1s are used to generate a quantum key distribution based on the BB84 protocol, as in the algorithm described in section 3.2. After obtaining the key, a "Hello" message is entered for encryption using the one-time pad method, as indicated in Equation (5). A lattice is created from encryption data (in this step, a ciphertext is converted into integers), and the lattice is obtained from this step. Finally, Babai's algorithm is applied finds the closest vector problem in the lattice (the output is a closed vector).

Quantum key distribution

A	1	1	0	1	1	0	0	0	0	0	0	0	0	0	1	0	0	1	1	0	1	0	0	0	1	1	1	0	0	1	1	0	0	1	0
A-b	x	x	+	x	x	+	+	+	+	+	+	+	+	+	+	x	x	+	x	x	+	x	+	+	+	x	x	x	+	+	x	x	+	+	x	+
A-P	\	\	|	\	\	|	|	|	|	|	|	|	|	\	/	|	\	\	|	\	|	|	|	\	\	\	|	|	\	\	|	|	\	|
B-b	x	x	+	x	+	+	+	+	+	+	+	+	+	+	x	+	+	x	x	+	x	+	+	+	x	x	+	+	+	x	x	+	+	x	+
B-p	\	\	|	\	-	|	|	|	|	|	|	|	|	\	-	|	\	\	|	\	|	|	|	\	\	-	|	|	\	\	|	|	\	|
key	1	1	0	1		0	0	0	0	0	0	0	0	0	1		0	1	1	0	1	0	0	0	1	1		0	0	1	1	0	0	1	0

Here,
A: Alice's random bit;
A-b: Alice's random sending basis;
A-p: Photon polarization sent by Alice;
B-b: Bob's random measurement basis; and
B-p: Photon polarization measured by Bob.

Key =

1	1	0	1	0	0	0	0	0	0	0	0	0	1	0	1	1	0	1	0	0	0	1	1	0	0	1	1	0	0	1	0

One-time pad encryption
Message = 'Hello'
= [72 101 108 108 111]; 'Hello' in decimals
Convert from decimals into binary vector

0	0	0	1	0	0	1	1	0	1	0	0	1	1	0	0	1	1	0	1	1	0	0	1	1	0	1	1	1	1	1	1	0	1	1

Ciphertext =

1	1	0	0	0	0	1	1	0	1	0	0	1	0	0	1	0	1	1	1	1	0	1	0	1	0	0	0	1	1	0	1

Create a lattice from encryption data.
In this step, convert the ciphertext into integer numbers. Create a lattice from these data.

Ciphertext in binary form:

1	1	0	0	0	0	1	1
0	1	0	0	1	0	0	1
0	1	1	1	1	0	1	0
1	0	0	0	1	1	0	1

Decimal Ciphertext = 195 146 94 177
Lattice = 195 94
146 177

Apply Babai's algorithm to find the closet vector problem in a lattice.
W= [203 456] Find the CVP in the lattice.
Lattice = V = 195 94
146 177
t = 2.1101 0.8176
round t
t = 2 1
v1 = 32 278
v2 =207 199
v = 239 477 This closet vector

X. CONCLUSION

Quantum cryptography promises to address some of the problems that have plagued classic encryption techniques, such as the main distribution problem and the expected collapse of the public / private key system. Quantum coding operates on the principle of Heisenberg's uncertainty and the random polarization of light. Another purely theoretical basis includes EPR entangled pairs. Given the high cost of implementation and the adequacy of current encryption methods, quantum cryptography is unlikely to achieve widespread use for several more years.

XI. CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest.

ACKNOWLEDGMENTS

This work was supported by the Islamic University under Grant No. RGIU2022.

REFERENCES

[1] L. Strate, "The varieties of cyberspace: Problems in definition and delimitation," *Western Journal of Communication*, vol. 63, no. 3, pp. 382-412, Sep. 1999. DOI: 10.1080/10570319909374648.

[2] V. Mavroeidis, K. Vishi, M. D. Zych, and A. Jøsang, "The impact of quantum computing on present cryptography," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 3, pp. 405-414, Mar. 2018. DOI: 10.14569/IJACSA.2018.090354.

[3] D. N. Diep, "Multiparty quantum telecommunication using quantum fourier transforms," *arXiv preprint arXiv:1705.02608*, May 2017. DOI: 10.48550/arxiv.1705.02608.

[4] A. Peres, *Quantum Theory: Concepts and Methods*, Springer Science & Business Media, 2006.

[5] J. Shen, T. Zhou, X. Chen, J. Li, and W. Susilo, "Anonymous and traceable group data sharing in cloud computing," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 4, pp. 912-925, Apr. 2018. DOI: 10.1109/TIFS.2017.2774439.

[6] M. Curty and D. J. Santos, "Quantum authentication of classical messages," *Physical Review A - Atomic, Molecular, and Optical Physics*, vol. 64, no. 6, pp. 6, Nov. 2001. DOI: 10.1103/PhysRevA.64.062309.

[7] B. S. Shi, J. Li, J. M. Liu, X. F. Fan, and G. C. Guo, "Quantum key distribution and quantum authentication based on entangled state," *Physics Letters, Section A: General, Atomic and Solid State Physics*, vol. 281, no. 2-3, pp. 83-87, Mar. 2001. DOI: 10.1016/S0375-9601(01)00129-3.

[8] D. Zhang and X. Li, "Quantum authentication using orthogonal product states," in *Proceedings of Third International Conference on Natural Computation*, Hainan, China, vol. 4, pp. 608-612, 2007. DOI: 10.1109/ICNC.2007.589.

[9] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science*, vol. 560, no. P1, pp. 7-11, Mar. 2014. DOI: 10.1016/j.tcs.2014.05.025.

[10] S. K. Routray, M. K. Jha, L. Sharma, R. Nyamangoudar, A. Javali, and S. Sarkar, "Quantum cryptography for IoT: APerspective," *2017 International Conference on IoT and Application (ICIOT)*, Nagapattinam, India, pp. 1-4, 2017. DOI: 10.1109/iciota.2017.8073638.

[11] K. A. Balygin, I. B. Bobrov, A. N. Klimov, S. N. Molotkov, and M. I. Ryzhkin, "A simple method of protection against a detector mismatch attack in quantum cryptography: The BB84 protocol," *Journal of Experimental and Theoretical Physics*, vol. 130, no. 2, pp. 161-169, Apr. 2020. DOI: 10.1134/S1063776120010136.

[12] P. Sazonova and S. Krendelev, "Parametric hash function resistant to attack by quantum computer," in *Proceedings of the 2018 Federated Conference on Computer Science and Information Systems*, Poznan, Poland, pp. 387-390, 2018. DOI: 10.15439/2018F254.

[13] J. Choi, S. Oh, and J. Kim, "The useful quantum computing techniques for artificial intelligence engineers," in *Proceedings of International Conference on Information Networking*, Barcelona, Spain, pp. 1-3, 2020. DOI: 10.1109/ICOIN48656.2020.9016555.

[14] K. Shannon., E. Towe, and O. K. Tonguz, "On the use of quantum entanglement in secure communications: A survey," *arXiv preprint arXiv:2003.07907*, Mar. 2020. DOI: 10.48550/arxiv.2003.07907.

[15] F. Xu, X. Ma, Q. Zhang, H. K. Lo, and J. W. Pan, "Secure quantum key distribution with realistic devices," *Reviews of Modern Physics*, vol. 92, no. 2, pp. 025002, Jun. 2020. DOI: 10.1103/REVMODPHYS.92.025002.

[16] P. D. M. Lara, D. A. Maldonado-Ruiz, S. D. A. Díaz, L. I. B. López, and Á. L. V. Caraguay, "Trends on computer security: Cryptography, user authentication, denial of service and intrusion detection," *arXiv preprint arXiv:1903.08052*, Mar. 2019. DOI: 10.48550/arxiv.1903.08052.

[17] S. Mitra, B. Jana, S. Bhattacharya, P. Pal, and J. Poray, "Quantum ryptography: Overview, security issues and future challenges," in *2017 4th International Conference on Opto-Electronics and Applied Optics*, Kolkata, India, pp. 1-7, Apr. 2018. DOI: 10.1109/OPTRONIX.2017.8350006.

[18] Z. Brakerski, R. Canetti, and L. Qian, "On the computational hardness needed for quantum cryptography," *arXiv preprint arXiv:2209.04101*, Sep. 2022. DOI: 10.48550/ARXIV.2209.04101.

[19] C. Portmann and R. Renner, "Security in quantum cryptography," *Reviews of Modern Physics*, vol. 94, no. 2, Jun. 2022, DOI: 10.1103/revmodphys.94.025008.

Abbas M. Ali Al-muqarm

Abbas M. Ali Al-muqarm received aBSc degree in computer science from the University of Kufa, Najaf, Iraq in 2013and anMSc degree in computer science from the Faculty of Computer Sciences and Mathematics, University of Kufa, Najaf, Iraq in 2020. He is currently a PhD candidate. His current research interests include Internet of Things, wireless sensor networks, mobile crowdsensing, cloud computing, and networking.

Firas Abedi

Dr. Firas Abedi received his PhD in information and communications engineering from Huazhong University of Science and Technology, Wuhan, China in 2019. He currently works as a lecturer at Al-Zahraa University for women, Karbala, Iraq. His research interests lie in source coding, wireless communications, and cryptosystems.

Ali S. Abosinnee

Ali Sahib Abosinnee received his BSc in 2014 and his MSc in 2020 in computer science from the University of Kufa, Najaf, Iraq. He currently works as a lecturer and the director of the world rankings unit at Altoosi University College, Najaf, Iraq. His current research interests include wireless communication, digital signal processing, computer vision, machine learning,and deep learning.