Design and Development of Quantum Computing based Protocols for Secure Internet of Things

A THESIS

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE AWARD OF THE DEGREE
OF

DOCTOR OF PHILOSOPHY

Submitted by

DIKSHA CHAWLA

(2K20/PHD/CO/502)

Under the supervision of

DR. PAWAN SINGH MEHRA

DEPARTMENT OF
COMPUTER SCIENCE AND ENGINEERING
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi 110042

MAY, 2024

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi-110042

CANDIDATE'S DECLARATION

I, Diksha Chawla (2K20/PHDCO/502) Research Scholar (Department of Computer Science and Engineering), hereby declare that the thesis titled **"Design and Development of Quantum Computing based protocols for secure Internet of Things"**, which is submitted by me to the Department of Computer Science and Engineering, Delhi Technological University, in partial fulfilment of the requirement for the award of Doctorate of Philosophy is original and not copied from any source without proper citation. This work has not previously formed the basis for awarding any Degree, Diploma, Associateship, Fellowship or other title or recognition.

Place: Delhi Diksha Chawla

Date:

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi-110042

CERTIFICATE

This is to certify that the work entitled **”Design and Development of Quantum Computing based Protocols for Secure Internet of Things”**, which is being submitted by **Ms. Diksha Chawla, Roll No. 2K20/PHD/CO/502** to the Department of Computer Science Engineering, Delhi Technological University for the award of the degree of Doctor of Philosophy is a record bonafide research work carried out by her under my supervision and guidance. She has fulfilled the requirements for the submission of this thesis. The contents of this thesis, in whole or in parts, have not been submitted for any other degree or diploma.

Place: Delhi Dr. Pawan Singh Mehra

Date: **SUPERVISOR**

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi-110042

ACKNOWLEDGEMENT

Be grateful when things go good and graceful when they go bad; as it is said, I feel immensely grateful when it comes to acknowledging my thanks to those who helped me complete my thesis successfully. At the onset, I bowed my head to the almighty God, who led me on this path, as everything has been possible with his blessings.

I take great pleasure in expressing my gratitude with profound respect to my revered supervisor, **Dr. Pawan Singh Mehra**, Assistant Professor, Department of Computer Science and Engineering, Delhi Technological University, New Delhi, for his invaluable guidance, close supervision, untiring ever, ready help and discussions throughout my Ph.D. work. I am indebted to him for his constructive criticism, exemplary patience, perseverance, motivation, and immense knowledge, which have gone a long way towards completing this thesis. His constant inspiration gave me considerable impetus to achieve this milestone. I could not have imagined having a better supervisor and mentor for my Ph.D. study.

I extend my gratitude to **Prof.(Dr.) Vinod Kumar**, Head, Department of Computer Science and Engineering, Delhi Technological University, New Delhi, for his support and guidance in carrying out this research work.

I also extend my heartiest thanks to the **Departmental Research Committee** for monitoring the progress and providing priceless suggestions encouraging me to widen my research from various perspectives.

I am also deeply grateful to all the members of the Department of Computer Science and Engineering, Delhi Technological University, for their constant help and providing all the necessary research resources.

I am also thankful to all academic, administrative and technical staff of Delhi Technological University for providing me with the university's resources and the necessary laboratory and research facilities for carrying out this work throughout my candidature.

A special thanks to my family members for their love, encouragement, patience and trust. With God's grace, this work allows me to make my parents, **Mr. Harish Chawla** and **Mrs. Ritu Chawla**, feel proud. I am also thankful to my lovely brother, **Mr. Kartik Chawla**. Their prayer for me was what sustained me in reaching this milestone.

Place: Delhi

Diksha Chawla
2K20/PHD/CO/502

Abstract

The Internet of Things (IoT) links numerous diverse devices, enabling a broad range of automation applications, including smart agriculture, smart home systems, and smart healthcare solutions, among others. Many classical solutions exist for user privacy, integrity, confidentiality and mutual authentication. The existing solutions are based on asymmetric and symmetric cryptographic schemes that are proven to be secure, and it is still used in many IoT-based applications for encryption. However, wireless communication channels face increasing security threats like data modification, man-in-the-middle, and Wi-Fi attacks, particularly as IoT becomes more widespread. The encryption methods need to be improved with the significant advancement of IoT communication. Classical cryptography establishes shared secret keys which are communicated over an insecure channel. Therefore, the main challenge is to find a method to distribute secret keys securely. The Quantum computing-based algorithms such as Shor's and Grover's, however, impose futuristic threats to classical public key and private key infrastructure. Shor's algorithm shows concerns about the security of the prime factorization-based cryptographic algorithm. The symmetric key structures, such as ciphers with short key sizes, hash functions with fixed-sized short hashes, and MAC authentication functions with short parameters, can be easily broken using Grover's algorithms. Thus, we need a better solution to mitigate the effects of both Classical and Quantum attacks.

Inspired by the evolution of cryptographic techniques from classical to Quantum cryptography, we analyzed to understand and adapt to this technological shift. Our focus was on achieving comprehensive end-to-end security. Secure Key Agreement (KA) and Mutual Authentication (MA) are essential for fortifying the IoT communication framework against conventional and potential future Quantum attacks. Therefore, in our proposed work, we aim to identify Quantum-based schemes to develop a Quantum-enabled IoT communication cryptosystem that can resist classical and Quantum attacks.

To achieve the abovementioned framework, we surveyed the 5G-enabled IoT communication framework. The existing attacks and classical cryptography-based solutions are also analysed. We investigated Quantum Computing and its impact on existing classical cryptographic schemes. We also examined the Quantum cryptography-based secure key distribution method in the survey. Our work also provides a comparative analysis of Quantum-based schemes with classical cryptographic measures.

To safeguard IoT communication against unauthorized access, it is inevitable to develop a security protocol that ensures the secrecy of keys and mutual authentication. Therefore, we designed a Novel Quantum Authentication and Key Agreement (QAKA) protocol that provides unconditional security against any classical and futuristic Quantum threats. In QAKA, each protocol ensures secure Key Agreement (KA) and Mutual Authentication (MA) based on Quantum hashing with Quantum Passwords (QP) and Quantum Key Distribution (QKD). The proposed scheme utilizes Quantum Teleportation and Greenberger-Horne-Zeilinger (GHZ) states for secure data transfer among entities. The proposed protocol is compared with the related protocols regarding various security features such as replay attacks, Man–in–middle attacks and futuristic Quantum attacks. The proposed protocol is implemented on IBM Quantum Experience (IQE), and simulation experiments have been performed for the designed protocol on Automated Validation of Internet Security Protocols and Applications (AVISPA). The performance of the proposed protocol is presented, revealing superior efficacy when juxtaposed with classical authentication schemes and Quantum protocols.

IoT-based healthcare systems are popular due to their ability to collect patient data and provide medical assistance. Therefore, for a secure IoT-based healthcare framework, a Quantum-based secure cryptosystem using mutual authentication for healthcare (QSMAH) protocol is proposed. It ensures secure Key Agreement (KA) and Mutual Authentication (MA) based on Quantum Cryptography. For secure data transmission, QSMAH utilizes Quantum Teleportation and Greenberger–Horne–Zeilinger (GHZ) states. Modified Quantum Key Distribution (QKD) is proposed for secure communication in QSMAH. The proposed protocol is implemented on IBM Quantum Experience (IQE), and simulation experiments have been performed for the designed protocol on Automated Validation of Internet Security Protocols and Applications (AVISPA).To prove the goal of our protocol, BAN logic is applied. The results reflect that QSMAH is also resistant to classical attacks and futuristic Quantum attacks on cryptographic schemes.

The comparative analysis of the proposed schemes with existing state-of-the-art solutions is presented in the thesis work. The performance of the proposed model is validated by considering the total number of hash operations, messages exchanged, the number of entities involved and sacrificed Qubits. The results indicate that the proposed platform with Quantum Key Distribution(QKD) and Greenberger-Horne-Zeilinger(GHZ) states is promising for securing resource-constrained IoT devices.

Keywords: Quantum Cryptography, Mutual Authentication, Internet of Things (IoT), Greenberger-Horne-Zeilinger(GHZ) state, Quantum Key Distribution (QKD), Quantum Teleportation.

Contents

List of Tables

List of Figures

List of Abbreviations and Symbols

Abbreviation	**Description**	**Abbreviation**	**Description**
IoT	Internet of Things	WSN	Wireless Sensor Nodes
COVID-19	Coronavirus disease	H2M	Human–To–Machine
OWS	Open Web Security	5G NR	5G New Radio
MA	Mutual Authentication	GWN	Gateway node
M2M	Machine to Machine	DES	Data Encryption Standard
D2E	Device to Everything	QGHIC	Quantum Green Health Identity-Card
QFT	Quantum Fourier Transform	QW	Quantum Walk
V2V	Vehicle-to-Vehicle communication	X	Position Operator
V2X	Vehicle-to-Anything	h	Plank's Constant
DoS	Denial of Service	AQDC	Authenticated Quantum Direct Communication(AQDC)
DDoS	Distributed Denial of Service	$\langle v \| \| v \rangle$	Bra-Ket Vector
MAC	Media Access Control	FFT	Fast Fourier transform
QBER	Quantum Bit Error Rate	QK-GRID	Quantum Key GRID
QWHF	Quantum Walk Hash Function	DI-QKD	Device-Independent QKD
CAQW	Controlled Alternate Quantum Walks	QRO	Quantum Random Oracle

List of Abbreviations and Symbols

Abbreviation	Description	Abbreviation	Description
Y	Pauli Y-Gate	CSWAP	Controlled SWAP Gate
EPR	Einstein–Podolsky –Rosen paradox Controlled SWAP Gate	I	Identity Gate
CCNOT	Controlled Control NOT	CNOT	Controlled NOT Gate
X	Pauli X-Gate	Z	Pauli Z-Gate
ID_{QSN}	Quantum Sensor Node Identity	$\wedge$	AND
QOWF	Quantum –One-Way Function	BB84	Bennett and Brassard
$\|V>$	KET-Vector	QGC	Quantum Green Card
QC	Quantum Cryptography	ψ	Wave Function
$\|\|$	Concatenation	$\otimes$	Tensor Product
<v |	BRA-Vector	$\|\Phi^{\pm}>$ and $\|\psi^{\pm}>$	Similar and Different Bell states
QSN	Quantum Sensor node	PQC	Post-Quantum Cryptography
ϕ	phi	QAC	Quantum Authenticated Channel
δ	delta	α and β	Complex probability amplitudes
ID_{USER}	User Identity	PW_{USER}	User Password
$\|+\rangle$ and$\|-\rangle$	H-Basis	MITM	Man-in-the-Middle
Qubit	Quantum Bit	C1,C0	Classical Bit string
AVISPA	Automated Validation of Internet Security Protocols and Applications	BAN	Burrows, Abadi and Needham
HLPSL	High-Level Protocol Specification Language	SATMC	SAT-based Model Checker
OFMC	On the Fly-Model Checker	CL- AtSe	Constraint Logic-based Attack Searcher
S	State	QP	Quantum Password

List of Abbreviations and Symbols

Abbreviation	Description	Abbreviation	Description
QSMAH	Quantum-based Secure Cryptosystem Using Mutual Authentication for Healthcare	TA4SP	Tree Automata based on Automatic Approximations for the Analysis of Security Protocols
GHZ	Greenberger–Horne–Zeilinger	OTP	One Time Password
QK	Quantum Key	SK	Session Key
QKD	Quantum Key Distribution	KA	Key Agreement
G()	Key generation Algorithm	P ∪ K	Public key
AKA	Authentication and key agreement	IQE	IBM Quantum Experience
AKD	Authenticated Key Distribution	AKE	Authenticated Key Exchange
Puk	Public key	Prk	Private Key
CMS	Central Medical Server	$\|CW >$	Codeword in the superposition state
RSA	Rivest Shamir Adleman	TS	Time Stamp
ECC	Elliptic Curve Cryptography	AES	Advanced Encryption Standard
BSN	Body Sensor Nodes	$\|+ >, \|- >$	H-Basis
$c_0, c_1, c_2.....c_n$	Classical Bits	$\|PW_P >$	User Patient
Qubit	Quantum Bit	$q_0, q_1, q_2.....q_n$	Quantum bits
$< Z\|$	BRA-Vector	$\|Z >$	KET-Vector
$\|ID_{GWN} >$	Gateway Node Identity	M^U_{SN}, M^U_{GW}	Measurement outcomes of Sensor Node and Gateway Node
$\|ID_{QSN} >$	Identity of Quantum Sensor Node	$\|ID_P >$	Identity of Patient
$\|ID_{MP} >$	Identity of Medical Professional	MP	Medical Professional

Chapter 1

INTRODUCTION

1.1 Internet of Things(IoT)

The rapid development of a new computing era termed the Internet of Things (IoT) has been the most advanced technological evolution. The IoT is an interconnected network of Sensors, Objects, and Gateways, giving IoT eloquent importance. The real-time information collected from sensors is processed through the gateway and communicated to clouds to facilitate users' decision-making. The IoT emergence has supported heterogeneous applications such as intelligent cities, green IoT-based agriculture, industry 4.0, E-healthcare, smart drones, smart vehicles, etc. The open nature of IoT systems makes the entire communication vulnerable to different security and privacy-related attacks. In such an environment, the attackers can execute active and passive attacks such as eavesdropping, insider, user impersonation attacks, GWN bypassing, traffic analysis, etc. Safeguarding sensitive data from smart applications against cyber threats is imperative. The current security infrastructure on the Internet is built upon asymmetric techniques[1]. Examples of such techniques include RSA and ECC, as discussed by [2], which rely on solving problems like integer factorization and discrete logarithms. This cryptographic approach is also applicable in securing Internet of Things (IoT) systems, as elucidated in recent overviews such as the one by[3]. Notably, networking protocols in IoT, like IEEE 802.15.4 and CoAP, incorporate security measures such as the Advanced Encryption Standard (AES), Elliptic Curve Cryptography (ECC), Elliptic Curve Digital Signature Algorithm (ECDSA), and Elliptic Curve Diffie-Hellman (ECDH). However, as per analysis[4, 5], these classical cryptographic schemes suffer from Man-in-the-Middle attacks, forgery attacks, replay attacks, insider attacks and sensor node impersonation attacks, etc. These classical cryptographic schemes must ensure basic security services such as mutual authentication, data confidentiality, integrity, non-repudiation and access control. The major difficulty is the resource-constrained architecture of IoT. IoT combines a heterogeneous collection of different technologies, devices and services with different security requirements. IoT devices are usually limited to memory and processing power. Some IoT devices have integration capabilities with large numbers of nodes leading to serious security issues. Hence, there is a need to formulate a security strategy tailored to suit all constrained environments within the Internet of Things (IoT).In addition, the evolutions of IoT communication from each sector, such as industrial or consumer, demand high security to protect their IoT devices from intrusion. In the next sections, IoT architecture security concerns,5G-enabled IoT, and IoT-based smart applications. The discussion revolves around Quantum Computing and its effect on the security of IoT.

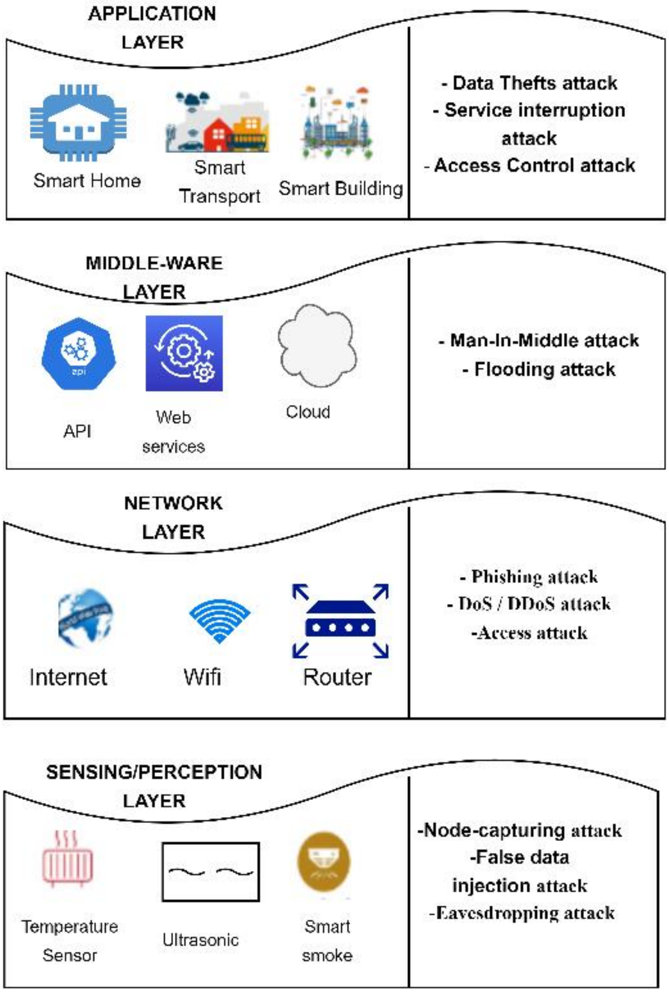


Figure 1.1: Layered Architecture of IoT

1.2 Architecture of the Internet of Things(IoT)

Inventive applications like smart agriculture, intelligent cities, and innovative healthcare have propelled the progress of IoT-enabled communication. The IoT devices that support these applications transmit vast amounts of data in many different environments. The advancement in IoT applications increases cyber-attacks. It also poses threats to user privacy and confidentiality. The main security challenges concerning the IoT environment are authentication, integrity, authorization and trust management. Major security concerns encountered in IoT layered architecture[6], as represented in Figure 1.1

1.2.1 Sensor Layer

This layer comprises intelligent smoke detection, temperature sensors and smart sensors for communicating with the network layer. The various sensors at this layer sense data from the environment to provide application decision-making capability. Therefore, authentication at this layer is important. It ensures that the data from a legitimate sensor node can be passed to the other layer for processing. Major sensor layer security issues that can be under this layer are as follows[7]:

a. **Booting Attacks**: such attacks occur because the inbuilt security process is not enabled during the booting process. Due to this, the edge devices became vulnerable, and the attackers may try to exploit this vulnerability. In most common cases, the attacker attacks the node devices when restarted. Thus, it is essential to secure edge devices during sleep-wake cycles.

b. **Sleep Deprivation Attacks**: In these scenarios, attackers attempt to deplete the energy of low-powered IoT edge devices by executing numerous loops with malicious code. Consequently, these nodes, now depleted, will disrupt services within the IoT application, leading to the presence of inactive nodes.

c. **Eavesdropping and Interference:** The assailants could seize the data and obtain confidential information during phases like data exchange or authentication due to the deployment of IoT in an open environment.

1.2.2 Network Layer

Within the IoT network stratum, technological accelerants involve low-energy expansive area networks (LPWAN). These LPWAN technologies, including IoT enablers, are instrumental in connecting crucial IoT applications. Nevertheless, significant security challenges arise at this layer during the transmission of information from the lower layer to the processing unit for further processing:

a. **Phishing Attacks:** If the user's credentials are breached, the IoT framework becomes susceptible to cyber threats. Such attacks usually occur when users try to access web pages.

b. **DoS / DDoS Attacks:** IoT applications also deal with this attack. The assailant overwhelms the target with numerous undesirable queries, which hinders the destination server. These unwanted requests disrupt services used by genuine users.

c. **Access Attacks:** In the foreseeable future, there will be rapid growth in IoT-enabled devices that continuously receive and transfer useful information. Data becomes highly vulnerable to access attacks in this environment, also called advanced persistent attacks (APT). This attack occurs when an intruder steals valuable information rather than causing damage to the network.

1.2.3 Middleware Layer

In this layer, essential components encompass persistent data storage, system queuing, machine learning, and more. Given the substantial volume of data generated by IoT, ensuring its security is imperative. Moreover, while offering diverse functionalities, this layer also introduces vulnerabilities to various attacks, including:

a. **Man-in-the-Middle Attacks:** If there is an adversary in the middle of the communication channel. Then they may control the communication process. In this attack, the entire process is done without any knowledge of the clients.

b. **Signature Wrapping Attacks:** The entire attack is performed by decrypting the signature algorithm. One popular attempt has been made on XML signatures. Taking advantage of vulnerabilities in the Simple Object Access Protocol, the attacker can either execute or alter eavesdropped messages.

1.2.4 Application Layer

Authentication is the prominent issue at this layer. The application permits access to the communication channel exclusively for authorized users. However, the security at this layer is complex because, in many applications, access is not limited to single users, for example, smart homes. These applications offer services to end-users. Noteworthy security challenges encountered include:

a. **Data Breaches:** In IoT-based communication, much Sensor Node-generated data are transient for decision making. These green-IoT-based applications are for the betterment of society. However, data privacy threats become bottlenecks for futuristic applications.

b. **Access Control Attacks:** Only legitimate users should have exclusive access to the account. An access control attack occurs when unauthorized entities gain entry to the data or account, exposing the entire vulnerability of the IoT application.

c. **Service Interruption Attacks:** This attack makes the communication network artificially too busy to respond, similar to DDoS. As a result, IoT applications deny many authorized users from performing any task.

1.3 5G-enabled Internet of Things

5G wireless technology is transforming and revolutionising every aspect of the future communication system. 5G technology is revolutionizing the global world with high-quality and quantity of data rates. As depicted in Figure 1.2, IoT using 5G infrastructure supports massive ultra-reliable Machine to Machine interactions, Device to Everything (D2E), Vehicle to Infrastructure(V2I) and Vehicle Pedestrian(V2P) to access real-time data. The 5G provides users with many benefits, such as high-speed data transfer and low latency, which enable users to gather critical information anytime and anywhere.

5G will open up newer possibilities in enabling intelligent devices to fulfil the enormous demand for futuristic IoT frameworks. Moreover, the 5G–IoT communication network will be faster, with more connecting devices supported in heterogeneous network environments[8]. According to Gartner[9], almost 57% of organizations are working on 5G to drive IoT Communication. 5G will aid IoT applications such as intelligent agriculture, intelligent environments, securities and emergencies. It is possible because of the improved latency and bandwidth. These applications will ride on the top of the 5G network, requiring more security to lock down the new devices and connections. IoT is an encouraging innovation to understand the perspective of associated living. The futuristic smart innovation of IoT supports many applications such as intelligent homes, intelligent e-health care sector, smart green IoT-based agriculture and smart industries [10].

The 3rd Generation Partnership Project (3GPP)[11] proposed 5G standards for Authentication and Key Agreement (5G-AKA). Such standards were proposed for future Narrow-Band Internet of Things (NB-IoT), which has evolved from traditional Long Time Evolution (LTE) Technology. Consequently, NB-IoT has been used in various application areas like smart agriculture, parking, asset tracking, remote meter reading, etc.[12]. The 5G connectivity pledged to provide high data speeds in the multi-Gbps range, along with Minimal delay and extensive network connectivity. The main issues associated with

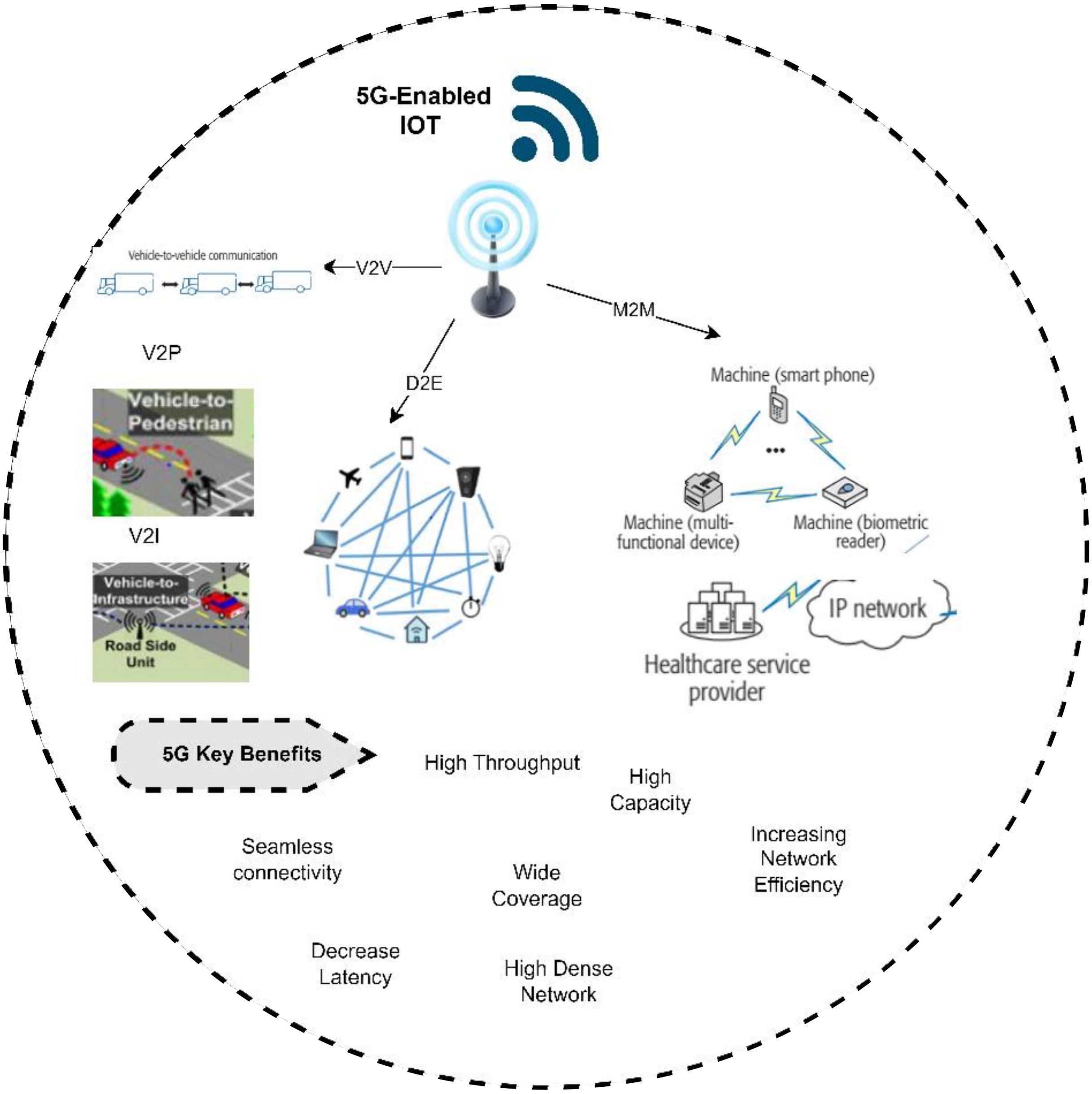


Figure 1.2: IoT, by enabling 5G benefits, supports massive ultra-reliable Device-to-Everything (D2E) and Vehicle-to-Everything (V2E) interactions.

5G radio access technology must be addressed, such as massive growth in connected devices and data traffic. 5G services can be categorized based on the connected services offered[13]:

(a) **Enhanced Mobile Broadband (eMBB):** 5G mobile technology can usher in new fascinating experiences by providing XR as the immersive experiences, with seamless connectivity of 5G and use of cloud services.

(b) **Mission-Critical Communication:** Such technology can provide services like vehicle-to-vehicle communication (V2V) and factory automation, providing high reliability and low latency.

(c) **Massive Machine Type Communication (mMTC):** This massive variety of interconnected devices. 5G enable a wide range of connectivity and coverage. It also connects low-cost battery-powered sensors, actuators, trackers, and wearables.

(d) **Ultra-Reliable low latency communication (URLLC):** This is system-centric, focusing on reliability and latency. The education sector could create virtual reality (VR)- -supported distance learning opportunities. 5G could allow doctors to squint into a patient's body using ultra-high-resolution imaging without cutting them in medical applications.

Therefore, current generations will be enhanced by transitioning to the next generation: 5G. Figure 1.3 represents specific 5G benefits that are required to be able to serve various smart devices and applications. It also represents the future high-performance targets as per International Mobile Telecommunications (IMT-2020) that 5G aims to achieve:

5G networks provide benefits to future IoT connectivity in comparison to 4G networks as discussed below[14]:

- Compared to the 4G/LTE network, a 100 times faster data rate is supported by 5G to support futuristic IoT applications.
- Currently, 4G supports a 100–150 Mb/s data rate; however, 5G provides approximately 10–32 Gb/s.
- Previously, in 4G, high latency issues arose in cloud computing; however, 5G associated with Fog computing (FC) reduces end-to-end (E2E) latency.
- The accessibility of D2D communication is increased due to 5G, as it enhances the battery power life by almost ten times.
- 4G supports low bandwidth, approximately 10 MHz; however, 5G supports higher bandwidth, approximately 60 GHz.

The three essential requirements for the physical design of NR are:

1. **Waveforms, Numerology and Frame Structure**
   NR waveform and numerology should be created by considering various link types. To support D2D communication, it provides uplink (UL), downlink (DL), sidelink and backhaul. It also provides support for vehicle-to-everything (V2X) communication. For waveform, numerology, frame structure, efficient time and frequency utilisation are necessary. As per 3GPP, 5G Orthogonal Frequency division multiplexing

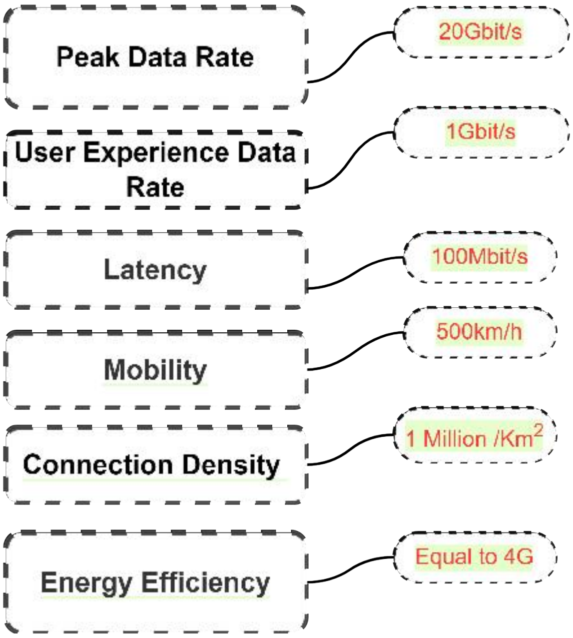


Figure 1.3: Performance Targets for 5G IoT as per IMT-2020

(OFDM) technology[8] has been introduced to support high spectral efficiency. This technology is proposed to meet high data rate requirements.

2. **Millimeter-wave**
   Millimeter-wave (mm-Wave) provide multi-gigabit communication services. It includes services such as high-definition television (HDTV) and ultra-high-definition video (UHDV)[15]. The huge bandwidth band from approximately 30 to 300 GHz has been supported by mm-Wave. Moreover, due to the continuous demand for mobile traffic, there is often a contradiction between spectrum shortage and capacity requirements. The tremendous spectrum provided to the fifth generation to fulfil the data demand of users of mm-Wave bands. Table 1.1 shows the difference between channel characterization of Line of Sight (LOC) and Non–Line of Sight (NLOC)[16].

Table 1.1: mm-wave propagation characteristics and applications in different frequency bands.

Frequency Band(GHz)	**Path Loss Exponent**		**Rain Attenuation**		**Applications**
	Line of Sight(LOC)	Non-Line of Sight(NLOC)	5 mm/h(db)	25 Mm/h(db)	
28	1.8-1.9	4.5-4.6	0.18	0.9	In-Band backhaul
38	1.9-2.0	2.7-3.8	0.26	1.4	Access and backhaul
60	2.23	4.19	0.44	2	HD video; access, backhaul and D2D; uplink channel access
73	2	2.45-2.69	0.6	2.4	Multimedia

3. **Massive Multiple-Input and Multiple-Output (MIMO)**
   It is utilized by 5G mm-Wave and provides high throughput and frequency reused

over a small distance, allowing efficient spectrum use. It increases cellular capacity and coverage by using many antennas.5G is specifically designed to support massive MIMO[12], using up to 256 antenna elements in the base station, limiting fitting antennas inside a mobile device. Therefore, MIMO enables intelligent beamforming, beam tracking and beam steering in spectrum bands under 6 GHz. It also enables a 5G mm-wave network to deliver high capacity and efficiency.

1.3.1 Recent Trends in 5G-enabled Internet of Things

In recent years, the increased spectrum of 5G has boosted the connection of many IoT devices[17]. Covering various manufacturers, industries, and consumer applications into a single model requires extensive network and standardization. However, 12 leading companies had already laid the foundation for 5G to boost automation and networking. The major players in the 5G-enabled IoT industry and their contributions towards implementing 5G-enabled IoT for the betterment of society are depicted in Table 1.2.

Table 1.2: Major industries in the 5G IoT industry

Research industries	**Contributions**
Samsung	Research on 5G technology was started by Samsung in 2011. Consider the company now one of the 5G domain leaders. Compared to current 4G network[8]. 5G provides data transmission several hundred times faster. Samsung provides an extensive contribution to the IoT platform. It lets users control home appliances like ACs, refrigerators, washing machines, etc. Some of the key developments of Samsung towards the 5G era: They developed a breakthrough in the 5G -ready antenna. and power amplifier technologies Samsung's Galaxy Watches with biometric sensors, military, heavy manufacturing, mining, etc., are future 5G applications that provide numerous IT solutions.
Huawei	Huawei realized recent advancements in the digital transformation of ICT network infrastructure. Therefore, investing a lot of amount into research focus on 5G wireless networks. The company is also patenting Key technologies. Some of the list activities of Huawei in the 5G domain: Provided intelligent Dual-Link features and ultra-high-speed broadband.
Qualcomm	Qualcomm R&D includes mm-wave antenna technology. The company also leads the overall 5G chipmaker and leads the 5G spectrum. Qualcomm is also progressing in designing and standardizing the new 5G, NR unified air interface. Key contributions towards 5G-enabled IoT: 5G new radio standards outdoor and multi-carrier aggregation boost signals into the Gbps range. They also contribute to cloud analytics virtualized core network functions.
Nokia	Recently, Nokia realized the need to provide robust network coverage with reduced cost. It also delivered: End-to-End network slicing functionality The fastest 5G speeds were achieved using the over-the-air (OTA) network.
NEC corporation	Their target is to do modifications in the industry according to the changing needs of organizations: They worked on the automation of the construction company. They devised a facial recognition demo system.
Cisco Systems	some developments made by the company: The company introduced a 5G security architecture. Support 5G services, infrastructure and automation.
LG	LG builds products that utilize the 5G networks rather than only deploying 5G networks. Some of the research work actively done by LG are: For an application such as in-vehicle infotainment specially designed for connected cars, LG announced an agreement with chipmaker Qualcomm.
Ericsson	As the company is proficient in the domain of 5G, many other big famous companies joined with Ericsson. Some of the research activities done by the company are listed as follows: Ericsson did the first 5Gdemonstration. The company is involved in almost all areas to make 5G a global standard for next-generation wireless technology.
ZTE Corporation	ZTE and its series solution propose the Pre5G concept.Key contributions by the company are: 5G new Radio air interface protocol proposed by ZTE. The company worked on applications requiring a 60 MHz spectrum, such as gigabit Ethernet without fibre connectivity, cloud XR, Autonomous driving and remote surgery.
Verizon	For 5G deployment to the world, it provides smart policies. In the 5G race, some of the contributions made by Verizon are: In four cities in late 2018, the company launched its 5G broadband internet.
Orange	The company contributes not only to smartphones but also to other content such as: Automated refrigerators, cars and augmented reality.

1.4 Smart Applications in Internet of Things

Deploying IoT applications poses challenges because of diverse environments and devices with limited resources. These applications must confront significant issues, including security and privacy concerns, both at the network and device levels, as emphasized by Li et al. in their work on 5G[9]. The subsequent sections delve into specific applications and the associated threats they encounter.

1.4.1 Smart Homes

A smart home embodies a technologically upgraded living environment, aiming to provide inhabitants with better standards of life. In the anticipated 5G-enabled IoT communication network of the future, billions of diverse devices are envisioned to be interconnected and engaged in mutual communication [18]. In an intelligent home environment, all connected devices increase malicious attacks[19]. The types of possible attacks and their possible countermeasures proposed by various authors are shown in Table 1.3. The Smart home attacks can be classified under two main categories:

Table 1.3: Security attacks and possible countermeasures in smart homes.

Security Attacks	**Countermeasures**	**Ref.**
Intrusion detection	Primary and Secondary access points in a home using different sensors	[20]
Replay attack	Symmetric key cryptography	[21]
Identity Protection	XOR and hash function	[22]

Passive attacks-It includes an eavesdropping attack without the consent of the communicating parties. The unauthorized interception of ongoing communication and traffic analysis are passive attacks. Hence, useful information from the adversary can be deduced by monitoring data traffic patterns. Such attacks do not modify data but learn useful information.

Active attacks- Such attacks modify user data. It includes masquerading attacks when an adversary pretends to be an authorized entity to gain special privileges. It also includes an attack such as replay in which an unauthorized person retransmits an originally captured message to produce an unauthorized effect.

1.4.2 Smart Farming

The latest progress in IoT technologies powered by 5G has transformed the strategies employed in smart agriculture. For example, preserving the privacy of IoT data aggregation has become crucial to safeguard the confidentiality of farmers' information while ensuring its availability[23]. Additionally, the agriculture sector, due to heterogeneous, internet-connected devices enabled by 5G IoT, has been exposed to potential cyber-attacks categorized as:

- **Data attacks**: include false data injection, insider and cloud data leakage and misinformation attacks.
- **Networking and equipment attacks**: side-channel, botnet, malware injection, DoS and radio frequency jamming.
- **Supply chain attacks**: includes third-party attacks and data fabrication attacks.

Many authors proposed different types of countermeasures for the attacks on smart agriculture sector, as represented in Table 1.4

Table 1.4: Smart agriculture possible attacks and countermeasures

Security Attacks	**Countermeasures**	**Ref.**
Replay	Feature-based biometric, Timestamp, pairing-based cryptography, hash functions.	[24]
Masquerade	Physiological-based biometric, hashing functions, ECC, and pairing- cryptography.	[25, 26]
Tracing	Random numbers in commitments.	[27]
Man-in-the-middle	Homomorphic encryption and hash functions: data aggregation schemes	[28]

1.4.3 E-Healthcare

The weaknesses of previous networks, ultra-low latency, high density, high bandwidth, high reliability, and high energy efficiency[17] are expected to be overcome by 5G. Due to advancements in technology, it supports E-healthcare applications [29]. Furthermore, wearable devices will facilitate conversations with doctors based on their data to alert those in the wider population if any health anomalies are detected [30]. 5G-enabled IoT supports real-time monitoring systems, necessary alerts and connectivity. Such devices help healthcare professionals be informed and ready during emergencies such as COVID-19, which can ultimately save many lives. Due to wireless connectivity, these systems are susceptible to security risks from unauthorized individuals. Descriptions of certain risks affecting e-healthcare systems include[26]:

- **Denial of Service-** The attacker tries to access secret patient data without authentication or permission.
- **Fingerprint and Timing-based Snooping** - In this scenario, the intruder tries to access information during data transient between sensors and from the sensor to a private user location. An intruder can disrupt a patient's health conditions by accessing such information.
- **Router attack**- As routing allows data to be delivered remotely and encourages network versatility, e-healthcare systems require data to be delivered securely and protect user identity. Extensive focus has been directed towards research in this domain, leading to developing multiple defence strategies against diverse healthcare sector threats. Several of these countermeasures are outlined in the Table 1.5.

Table 1.5: E-Health care possible attacks and countermeasures

Attacks	**Countermeasures**	**Ref**
Cross-Site Scripting (XSS) attack	Flirting method to prevent XSS attack.	[31, 32]
	Machine learning-based XSS detection system.	[31, 33]
SQL Injection Attack	Filtering all user input, data sanitization and ignoring creating SQL queries with user data.	[31, 34]
	Tokenizing-comparing model	[35]
DDoS attack	Healthcare environment - Traceback technique	[36]
Path-based DoS Attack	Anti-Reply protection and packet authentication	[37]
Data access attack	Game-theoretic model	[38]

1.4.4 Industrial IoT (IIoT)

Industry 4.0, IoT will offer unceasing connectivity and standard communication protocol solutions to existing industrial systems[39]. Therefore, it provides promising transformation to existing IIoT problems. IIoT is applied in automobile manufacturing, engineering machinery, refrigeration equipment, metal smelting, etc. The IIoT creates a strong requirement to safeguard important industrial applications from cybersecurity attacks.

Some of the possible attacks in IIoT are[36]: Masquerade, Virus, Trojan Horse, Worms, Cinderella, and Fragmentation. Table 1.6 shows some existing countermeasures for security threats in the IIoT framework.

Table 1.6: Attacks on IIoT and Possible Countermeasures

Cyber Threats	**Countermeasures**	**Ref**
Phishing attacks	Early analysis of phishing attacks and PHONEY for auto-detection.	[40]
	Intelligence Web Application Firewall (IWAF).	[41]
	Botnets Detection	[42]
Ransomware attacks	Futuristic firewalls - ameliorate traffic filtering capabilities.	[43]
	proposed application-specific machine learning algorithms.	[44]
	Intrusion detection system	[45]
Jamming DoS attacks	Data diversion to alternative routes	[46]
Collision attacks FHSS	The frequency-hopping spread spectrum (FHSS) is utilized to alleviate the interference.	[47]
Data transfer attacks	Data encryption techniques Datagram transport compressed protocol.	[48]
Supply Chain Attacks	Artificial intelligence (AI) and real-time intelligence, self-adapting supply chain systems using machine Learning (ML) for predictive cyber risk analytics.	[49] [50]

1.4.5 Smart Transportation

1.4.5.1 Vehicle Telematics

The field of Automotive and Transportation (A and T) already encompasses vehicle diagnostics, location tracking, and telematics applications. These applications support non-real-time data. However, real-time information about the situation and performance of the vehicle could easily be collected using 5G. Due to its enhanced speed and low latency, future applications can collect driver behaviour and validate the delivery of more state-of-the-art services.

1.4.5.2 Vehicle Infotainment

It is one of the futuristic applications that boosts the use of 5G. Some examples of the services offered by vehicle infotainment are in-car retail and marketing, AR/VR-based navigation systems and entertainment services. It additionally facilitates its utilization of external payment services like fuel payments. In the case of autonomous vehicles such as V2X communication, it is complex to ensure targeted functionality. Nonetheless, as a result of diverse connectivity, these applications could also be susceptible to the security risks listed in Table 1.7 as:

Table 1.7: Attacks on smart transportation and countermeasures.

Security Attacks	**Countermeasures**	**Ref**
Sybil attack	Cryptographic solutions	[51]
Falsified entities attack	Authentication	[52]
Replication attack	Key Management	[53]
Jamming attack	Anti-Jamming Techniques	[51]
Wormhole attack	Restriction on Packet transmission distance	[54]
Jamming attack	Detection of malicious component	[51]

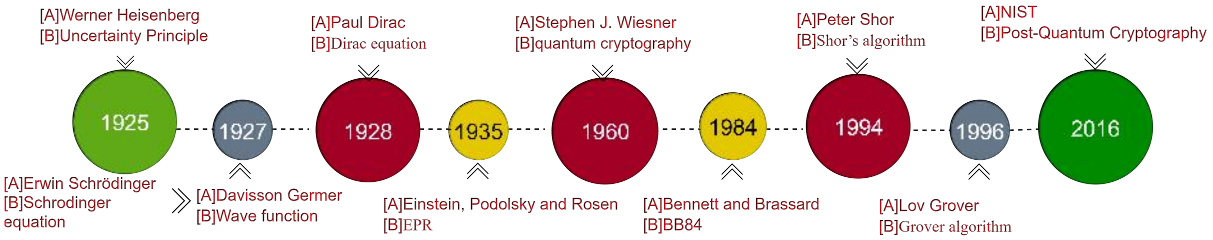


Figure 1.4: Significant development in Quantum computing theories [A-Inventor; B-Significant contribution.

1.5 Quantum Computing

Quantum information and computing were introduced by the famous American theoretical physicist Feynman[55] in the 1980s. However, the field gained attention after the article ‘Simulating Physics with Computers[53]. Even before that, in the late 1960s, Stephen J. Wiesner[54] started work on Quantum cryptosystems. Later, Charles H. Bennet and Gilles Brassard[56] did the practical implementation of Quantum computing-based protocols in 1984. They examined the principles of Quantum physics and information theory, leading to the creation of Quantum Computing. They proposed their first protocol based on Quantum mechanics known as BB84[57]. Figure 1.4 represents remarkable progress in Quantum computing and information. It represents the significant work done by researchers in Quantum computing, starting from the famous Heisenberg uncertainty principle towards the Post-Quantum cryptography era.

The IoT applications include intelligent cities, IoT-based green agriculture, E-healthcare, UAV, and many more. The advancement of these applications connects many IoT devices by using the internet. However, Quantum algorithms jeopardized the security of classical security protocols[52] based on mathematical structures. An emerging paradigm of Quantum information and computing has created an unsafe environment for the current security algorithms, which are extensively utilized to secure the IoT communication framework. Therefore, Quantum techniques are required to provide security to current and futuristic IoT devices. These techniques must be implemented to solve security breaches. In the next subsections, Quantum Computing fundamentals are discussed.

1.5.1 Qubits

A bit in classical computing is in the form of 0,1, representing a unit of information. In Quantum Computing, qubits are used to represent Quantum information. Qubits are the Quantum version of a bit; they can take the value $|0>$ and $|1>$ or a linear combination of both; the idea is known as superposition. A collection of n qubits can simultaneously be in an arbitrary superposition of up to 2^n different states. The superposition allows Quantum states to be indeterminate. Qubits are represented on the Bloch sphere. Mathematically, qubits are represented by a vector of length one in a two-dimensional complex vector space. The state vector in Quantum needs to be normalized as $<\psi|\psi>=1$. Thus if $|\psi>=\alpha|0>+\beta|1>$ then $\|\alpha\|^2 + \|\beta\|^2 = 1$ Quantum Qubits are single qubit $|0>=\begin{pmatrix}1\\0\end{pmatrix}$ and $|1>=\begin{pmatrix}0\\1\end{pmatrix}$ however, the multi-Qubit system can be generated using the tensor product as in Eq.1.1

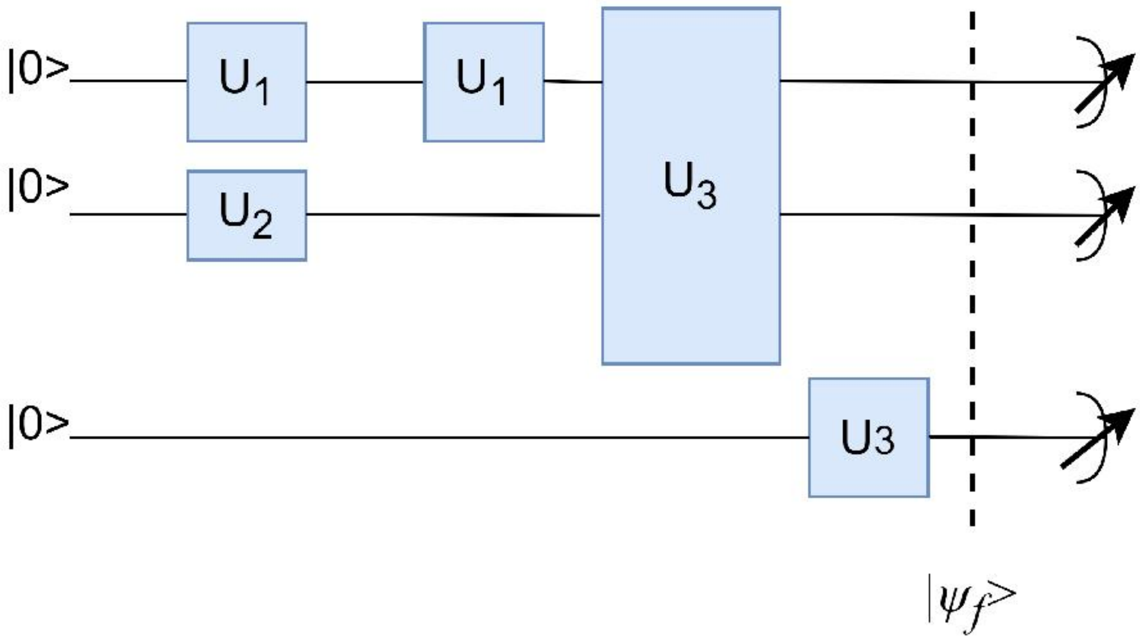


Figure 1.5: A Quantum Circuit. The $3 - \mathit{Qubit}$ state $(|0\rangle|0\rangle|0\rangle)$ using Quantum gates transformed into the final Quantum output state as $|\psi_f\rangle$ (f: final state).

$$|00\rangle = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}; |01\rangle = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}; |10\rangle = \begin{pmatrix}0\\0\\1\\0\end{pmatrix}; |11\rangle = \begin{pmatrix}0\\0\\0\\1\end{pmatrix} \tag{1.1}$$

1.5.2 Quantum Gates

Quantum transformation describes the mapping from the state space of a Quantum system to itself. The random transformation of a Quantum system is not possible. The linear transformations of the vector space describe these transformations as Eq1.2:

$$U(\alpha_1|\psi_1\rangle....\alpha_k) = \alpha_1 U|\psi_1\rangle + ...\alpha_k U|\psi_k\rangle \tag{1.2}$$

In Quantum Computing, qubits can be manipulated using Quantum gates. The Quantum gate, when applied to the Quantum state, will transform that state unitarily up until the point at which a measurement is made. As represented in Figure 1.5, the measurement on a computational basis provides the circuit output.

Quantum gates are single and multi-qubits, as represented in Table1.8. The single qubit transformation of gates is as follows:

1. X-Gate
   This gate is also called a negation gate. The X-Gate is utilized for single-qubit operations and can be used to flip the input state: $\sigma_x|0\rangle to|1\rangle$ and from $\sigma_x|1\rangle to|0\rangle$.

2. Y-Gate
   The Y-Gate performs the bit-flip operation like the X-Gate when the qubit is not in

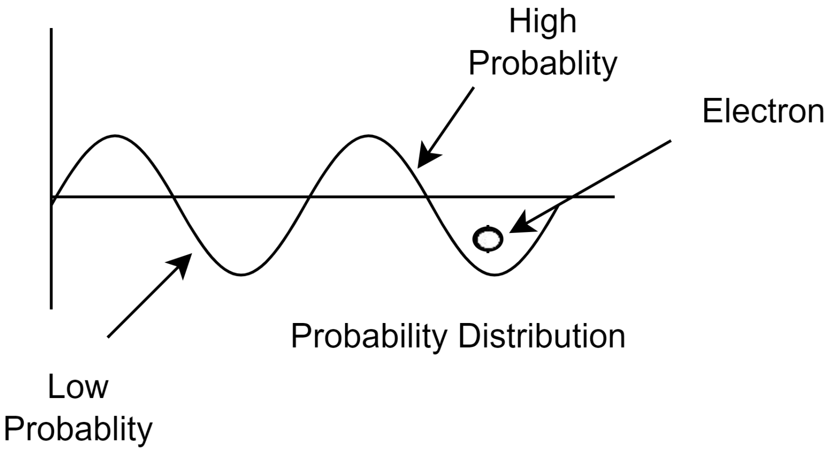


Figure 1.6: Particle-Wave Duality

superposition. However, when the qubit is in superposition, the Y-Gate performs a phase flip. Therefore, Y-Gate flips the phase from $+1 to -1$ or $-1 to +1$.

3. Z-Gate
   This gate is also referred to as the phase gate and is used to change the phase of the state. The Z-Gate gate without superposition will remain in the same state $\sigma_z|0\rangle = |0\rangle$ However, with superposition, the Z-Gate behaves like a phase gate and convert $\sigma_z|1\rangle = -|1\rangle$.

4. Controlled NOT (CNOT) Gate
   CNOT-Gate is a multi-quit gate called the Feynman gate. These gates are used for generating entangled states. Two input states represent the CNOT-Gate; the first control and second target qubit. If the first qubit is $|1\rangle$, it will flip its state.

5. Controlled Controlled-NOT (CCNOT) Gate
   CCNOT-Gate is a multi-qubit gate called, also called Toffoli gate. The Toffoli gate is based on dual controlled conditions. A Toffoli gate takes two input qubits and flips the value of the resulting qubit if the two input qubits hold a value of 1.

1.5.3 Wave Function

The Quantum state representation (Wave)is mathematically described as Ψ The wave defines the characteristics of a particle. The principle is based on Particle-Wave Duality. This probability is proportional to the value of ψ^2. Electrons move somewhere in the waveform area, which we do not know exactly about particles. However, what we know is only about probabilities. Certain mathematical operations are then applied to such a form of a particle, due to which, even if an adversary tries to copy data, it becomes impossible. The experiment that confirms the particle Wave duality is the Double-slit experiment[58]. Figure 1.6 represents the probability distribution of electrons. The high and low probability represents the value of the wave function of a particle at a given point of space and time is related to the likelihood of the particle's being there at the time.

Table 1.8: Single and Multiple Qubits Quantum Gates

Quantum Gates	**Matrix Representation**	**Circuit Representation**	**State representation**	**Single/ Multi-Qubit**	**Universal Reversible gates**	**Rotation**
X	X $= [\begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix}]$	ADD Circuit	Input: $\|\phi >= \alpha\|0 > +\beta\|1 >$ Output: $\|\phi >= \beta\|0 > +\alpha\|1 >$	Single	No	No
Z	Z $= [\begin{matrix} 1 & 0 \\ 0 & -1 \end{matrix}]$	ADD Circuit	Input: $\alpha\| > +\beta\|1 >$ Output: $\|\phi >= \alpha\|0 > -\beta\|1 >$	Single	No	Yes
H	H $= \frac{1}{\sqrt{2}}[\begin{matrix} 1 & 1 \\ 1 & -1 \end{matrix}]$	ADD Circuit	Input: $\|0 >$ and $\|1 >$; Output: $\alpha\frac{\|0>+\|1>}{\sqrt{2}}$ and $\beta\frac{\|0>-\|1>}{\sqrt{2}}$	Single	No	Yes
S	$R^z_{\pi/2} = [\begin{matrix} 1 & 0 \\ 0 & e^{\pi i/2} \end{matrix}] = [\begin{matrix} 1 & 0 \\ 0 & i \end{matrix}]$	ADD Circuit	Input: $\|0 >$ and $\|1 >$; Output: S$\|0 >\rightarrow \|0 >$;S $\|1 >\rightarrow i\|1 >$	Single	No	Yes
S†	$R^z_{3\pi/2} = [\begin{matrix} 1 & 0 \\ 0 & -i \end{matrix}]$	ADD Circuit	Input: $\|0 >$ and $\|1 >$; Output: S$^\dagger\|0 >\rightarrow \|0 >$, S$^\dagger\|1 >\rightarrow -i\|1 >$	Single	No	Yes
T	$R^z_{\pi/4} = [\begin{matrix} 1 & 0 \\ 0 & e^{\pi i/4} \end{matrix}]$	ADD Circuit	Input: $\|0 >$ and $\|1 >$; Output: T$\|0 >\rightarrow \|0 >$;T $\|1 >=$ e $^{i\pi/4}\|1 >$	Single	No	Yes
T†	$R^z_{7\pi/4} = [\begin{matrix} 1 & 0 \\ 0 & e^{7\pi i/4} \end{matrix}]$	ADD Circuit	Input: $\|0 >$ and $\|1 >$; Output: T$^\dagger\|0 >= \|0 >$, T $^\dagger\|1 >=$ e $^{-i\pi/4}\|1 >$	Single	No	Yes
CNOT Or Feynman	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$	ADD Circuit	Input $\rightarrow$ Output: If a = 1 then b = $\bar{b}$ $\|00 >\rightarrow \|00 >$, $\|01 >\rightarrow \|01 >$, $\|10 >\rightarrow \|11 >$, $\|11 >\rightarrow \|10 >$	Multi-Qubit	No	No

Quantum Gates	**Matrix Representation**	**Circuit Representation**	**State representation**	**Single/ Multi-Qubit**	**Universal Reversible gates**	**Rotation**
C-SWAP Or Fredkin	$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$	ADD Circuit	Input $\rightarrow$ Output: If CB = 1 then swap b and c $\|000 > \rightarrow \|000 >$, $\|001 > \rightarrow \|001 >$, $\|010 > \rightarrow \|010 >$, $\|011 > \rightarrow \|011 >$, $\|100 > \rightarrow \|100 >$, $\|101 > \rightarrow \|110 >$, $\|110 > \rightarrow \|101 >$, $\|111 > \rightarrow \|111 >$	Multi-Qubit	Yes	No
SWAP	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$	ADD Circuit	Input $\rightarrow$ Output: $\mathrm{U}_s\|\psi,\ \phi\ >= \mathrm{U}_s(\|\psi > \otimes\|\phi >) = \|\phi, \psi >$	Multi-Qubit	No	No
Toffoli Or CCNOT	$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$	ADD Circuit	Input $\rightarrow$ Output: If ab = 1 then c = $\overline{c}$ $\|000 > \rightarrow \|000 >$, $\|001 > \rightarrow \|001 >$, $\|010 > \rightarrow \|010 >$, $\|100 > \rightarrow \|100 >$, $\|110 > \rightarrow \|111 >$, $\|001 > \rightarrow \|011 >$, $\|101 > \rightarrow \|101 >$, $\|111 > \rightarrow \|110 >$	Multi-Qubit	Yes	No

1.5.4 Heisenberg Uncertainty Principle

The main logic behind this is a wave function that contains all of the positions of the moment of the electron. It will give us probability distribution; electrons always exist in different places with different probabilities for a specific wave. The probabilities create uncertainty in the Quantum system. Due to uncertainty, measuring a particle's position and momentum is impossible. Measurement creates a disturbance in the Quantum system. Therefore, the uncertainty principle is useful for Quantum Computing. It protects user data and communication networks from eavesdropping attacks[59]. Furthermore, multiplying the errors (represented as the delta in front of X and P) in the observation of these points has to give a value greater than or equal to half of a constant called "h-bar" as in Eq1.3:

$$\Delta X \Delta P \geq \frac{\hbar}{4\pi} \tag{1.3}$$

X is the position operator, P is the photon's momentum, and $\hbar$ is the plank's constant.

1.5.5 No Cloning Theorem

In 1982, Wootters, Zurek, and Dieks(WZD)[59] theoretically stated that there are only two ways to manipulate the composite system. One is through observation, and the other is by controlling the Hamiltonian of the system. The No-cloning theorem provides the safety of data transient in between the sensor node and GWN[60]. Due to No-cloning, an authenticated user will likely detect any disturbance in the Quantum system.

Suppose an exact Quantum state can be cloned. In that case, an eavesdropper could tap a Quantum channel, forward perfect copies of the qubits to the intended recipient, and examine the important information. Such exact Quantum copying is impossible. Figure 1.7 depicts the diagrammatic representation of the cloning of an arbitrary Quantum state[61]. The universal Quantum cloning machine, U_{clone} on an arbitrary pure state as in Eq.1.4

$$|\psi\rangle_A|0\rangle_B \xrightarrow{U_{clone}} |\psi\rangle_A|0\rangle_B \tag{1.4}$$

Here, the first particle (A) starting state is $|\psi\rangle$ and the second particle (B) starting state is $|0\rangle$ as in Eq.1.4. Considering an arbitrary state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

The target is to determine whether the clone of the Quantum state is possible or not, as in Eq1.5. If cloning changes the state, $|\psi\rangle$ is replicated on particle B. However, the results in Eq.1.6 show that the states are not the same.

$$(|\psi\rangle_A \otimes |0\rangle_B) \overset{?}{=} |\psi\rangle_A|\psi\rangle_B \tag{1.5}$$

L.H.S $QG(|\psi\rangle_A \otimes |0\rangle_B) = QG(\alpha|00\rangle + \beta|10\rangle)$
Therefore,$|\psi\rangle_A|0\rangle_B = \alpha|00\rangle + \beta|11\rangle$
However, RHS: $|\psi\rangle_A|\psi\rangle_B = \alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle$

$$QG|\psi_0\rangle|0\rangle \neq |\psi\psi\rangle_{AB} \tag{1.6}$$

1.5.6 Superposition

Quantum information bit, known as Qubit, is the foundation for Quantum Cryptography[59]. The classical binary bits 0 and 1 in Quantum are called Qubits [62]. Qubits can have a

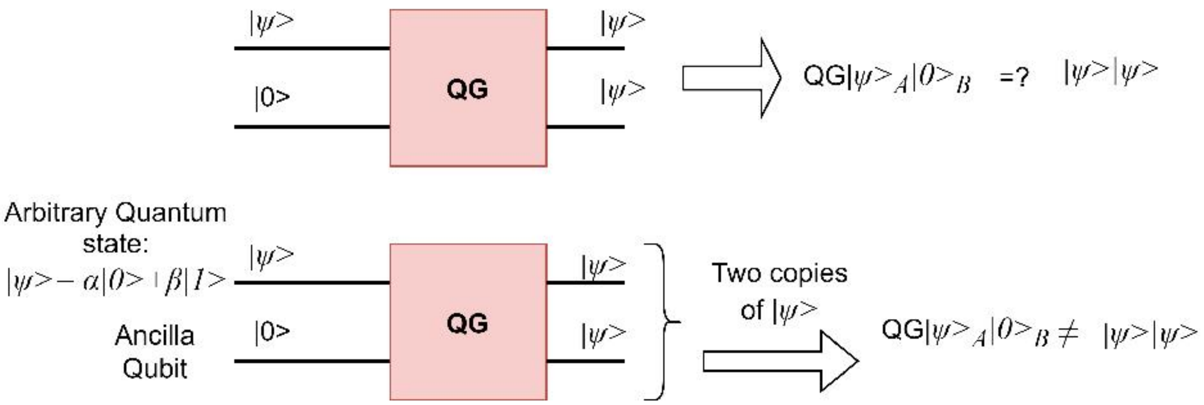


Figure 1.7: (a) represents whether the input state $|\psi\rangle$ using ancilla qubit $|0\rangle$ when processed through Quantum gate produces output state $|\psi\rangle$and $|\psi\rangle$(similar copy of qubit);(b) represents that creating identical copies of the same state is impossible.

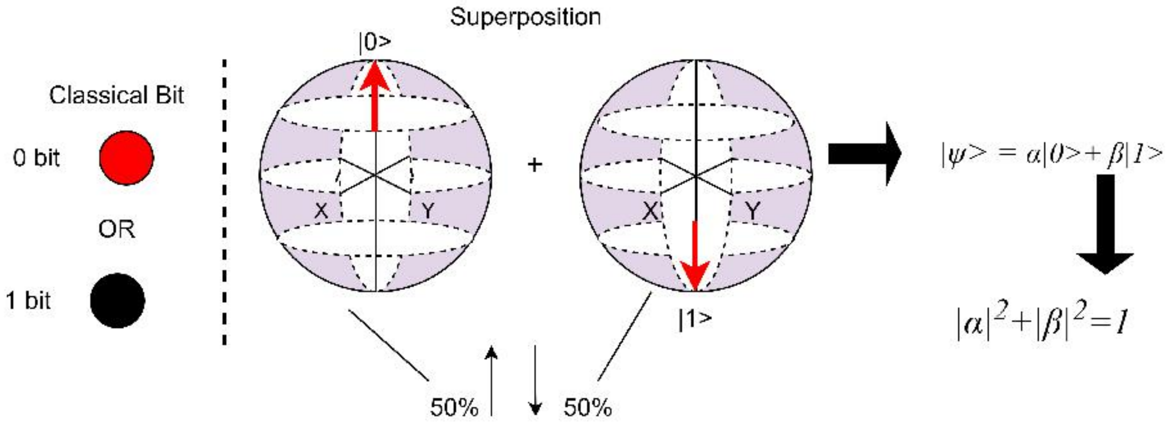


Figure 1.8: : Classical information: Bit(Left) and Quantum information: qubit(Right).

value of $|0\rangle$, $|1\rangle$ or any linear combination in between. The entire state is represented by $|\psi\rangle$. The α and β are the complex numbers. They represent the probability of being in state $|0\rangle$ or $|1\rangle$ as in Figure 1.8. The state of the Qubit can be represented as a vector and a Bloch sphere.The superposition allows us to solve computationally difficult problems by providing access to many dimensions of working memory that were unavailable to a classical computer.

Mathematically, Qubit are represented as a linear combination of vectors $|0\rangle$ and $|1\rangle$ in $\mathbb{C}$ as in Eq1.7:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle. \tag{1.7}$$

Two qubits in the superposition state are represented as :$\mathbb{C}^2 \otimes \mathbb{C}^2$

$$\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \tag{1.8}$$

Here, α and β represent probability amplitude and are complex numbers as represented in Eq.1.8. These complex numbers must satisfy the normalization conditions: $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2$

Through measurement, Qubit collapse to $|00\rangle, |11\rangle, |01\rangle$ or$|10\rangle$

1.5.7 Entanglement

It is a property that makes detecting intruders in network communication easy. When the simple independent probability multiplication rule does not work in identifying the exact probability value that means the particles are not independent. They are entangled. The changes in one state will affect the other state[63]. The local measurement will not work in entanglement. The only way to compute these bits is by joint operation. Two Quantum systems interact in such a way as to link both their spatial coordinates in a certain direction and their linear momenta (in the same direction). The phenomenon of entanglement creates the possibility of connecting particles widely separated in spaces. Entanglement is the teleportation feature that happens in composite systems and is absent in single-state systems[64]. The main concept of teleportation[56] is establishing a secure communication channel between two parties even without Quantum communication channels[65]. By utilizing Quantum teleportation, these entangled bits are shared among communicating parties. Entanglement is also referred to as Bell-states. There are four of them as in Eq1.9, which represent similar entanglements and Eq1.10, which represent different entanglements:

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle); |\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \tag{1.9}$$

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle); |\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{1.10}$$

1.5.8 Teleportation

The principle of No-cloning ensures that it is impossible to copy the Quantum state. Therefore, when one entity wants to send some message to another communicating party, it uses the process of Quantum Teleportation, as represented in Figure 1.9. Quantum teleportation is used to share messages between legitimate entities. Both entities use correlated (entangled bell) pairs as the connection and transfer mechanism. The message M is in a pure Quantum state,$|\psi\rangle_1$= $\alpha|0\rangle_1$+$\beta|1\rangle_1$, which is unknown to B. Using entanglement sender retains one of her Qubit and sends the other to the receiver. The two-particle entanglement where the sender correlates with receiver qubits as in Eq1.11:

$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle_{23} - |10\rangle_{23}) \tag{1.11}$$

Here, particles labelled 2 and 3 are entangled; however, particle 1(Message) is not. However, the three particles entangled system is as in Eq1.12:

$$|\psi_{init}\rangle = |\psi\rangle_1 \otimes |\beta_{11}\rangle_{23} \tag{1.12}$$

The overall state can be described in Eq1.13:

$$|\psi_{init}\rangle_{123} = \frac{1}{2}(|\beta_{11}\rangle_{12}(\alpha|0\rangle_3 + \beta|1\rangle_3) + |\beta_{01}\rangle_{12}(\alpha|0\rangle_3 - \beta|1\rangle_3) + \\ |\beta_{10}\rangle_{12}(\alpha|1\rangle_3 + \beta|0\rangle_3) + |\beta_{00}\rangle_{12}(\alpha|1\rangle_3 - \beta|0\rangle_3) \tag{1.13}$$

Next, the sender measures her part of the Qubit and the message Qubit he wants to communicate to the receiver. Alice then sends the result of her output measurement as

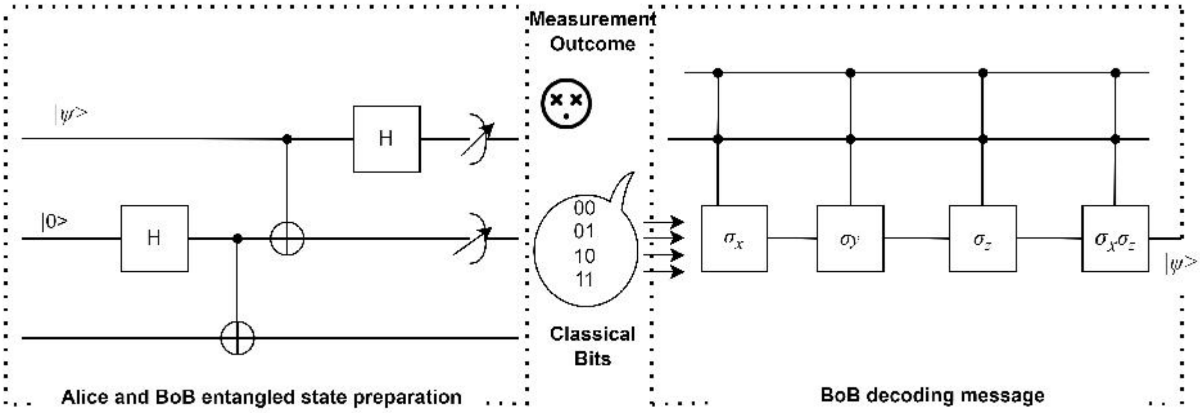


Figure 1.9: Quantum entangled state (Left) and resulting Quantum message by applying Quantum Gates (Right).

two classical bits to BOB as $00, 01, 10, 11$. Upon receipt, Bob then applies corrective gates to retrieve the appropriate message outcome $|\psi\rangle_1 = \alpha|0\rangle_1 + \beta|0\rangle_1$ The Quantum gates used by Bob to correct the output state are 00 → No action to be performed; 01 → apply an X rotation ; 01 → apply an X rotation; 10 → apply a Z rotation;11 → apply Z followed by X rotation

1.6 Impact of Quantum Computing on Internet of Things

Although Quantum computing has enormous potential, the field is still in its nascent age. IBM's practical implementation of Quantum computers is up to 127 qubits[66], but its evolution is already threatening cybersecurity. The security structure of IoT is based upon symmetric[67, 68, 69]and asymmetric[70, 71] cryptosystems. These cryptographically secured systems rely on the key distribution method. In the IoT framework, all key management and distribution are done over an insecure channel. Hence, it is difficult to identify authorized users. Quantum Computing algorithms hugely impacted the present security structure of IoT communication systems. Hence, there is an urgency to develop Quantum-resistant cryptosystems. Figure 1.10 represents the classification of public and private key cryptographic algorithms [12]. We have mentioned the impact of Quantum computing algorithms on these cryptographic schemes. Two Quantum algorithms that will execute on Quantum Computers[72] and are theoretically proven to break the security structure of classical algorithms are:

1.6.1 Shor's Algorithm

The highly complex integer factorization problem was solved by a famous mathematician Peter Shor[57]. The author published his work in 1994. His theory is experimentally demonstrated in Bell Laboratories. Later he showed his contribution to solving the elliptic curve discrete logarithm problems. Quantum Computing and algorithms hugely impacted classical public-key systems. The Diffie-Hellman (DH) key exchange, RSA and ECC algorithms are not secure with advancements in Quantum Computing and information. The algorithms mentioned above are based on the complexity of finding solutions to

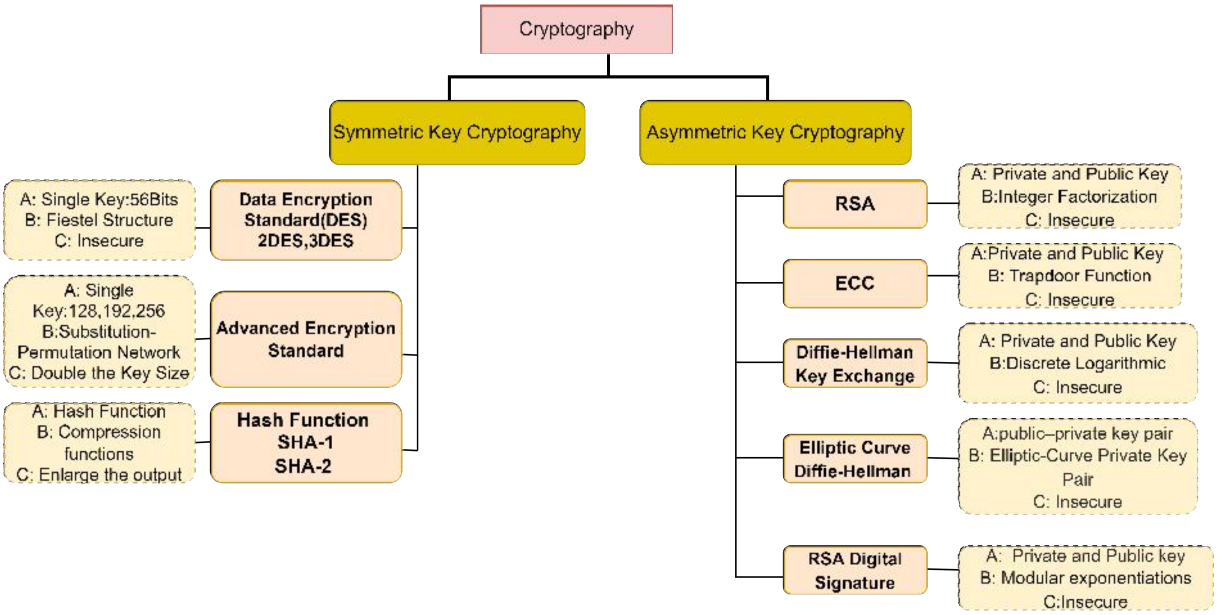

Cryptography
Symmetric Key Cryptography
Asymmetric Key Cryptography
A: Single Key:56Bits
B: Fiestel Structure
C: Insecure
Data Encryption Standard(DES) 2DES,3DES
A: Single Key:128,192,256
B:Substitution-Permutation Network
C: Double the Key Size
Advanced Encryption Standard
A: Hash Function
B: Compression functions
C: Enlarge the output
Hash Function SHA-1 SHA-2
RSA
A: Private and Public Key
B:Integer Factorization
C: Insecure
ECC
A:Private and Public Key
B: Trapdoor Function
C: Insecure
Diffie-Hellman Key Exchange
A: Private and Public Key
B:Discrete Logarithmic
C: Insecure
Elliptic Curve Diffie-Hellman
A:public–private key pair
B: Elliptic-Curve Private Key Pair
C: Insecure
RSA Digital Signature
A: Private and Public key
B: Modular exponentiations
C:Insecure

Figure 1.10: (a) Quantum computing impact on symmetric and (b) asymmetric cryptographic systemsA: Key Pair; B: Key Factor, and C: Quantum Computers impact on these algorithms.

problems such as integer factorization and discrete logarithms[73]. These systems operate under the One-Way Function (OWF). These functions had the property that they are easy to compute one way but difficult another way[55]. However, the Quantum shor's algorithm[74]resolved the problem of integer factorization in polynomial time[75]. Therefore, as soon as Quantum-based Shor's algorithm is implemented, many cryptographically secure systems that rely on prime number factorization problems will become insecure. For example, Quantum Shor's[57] algorithm gave an approximately 80% probability[74]that the value of the divisor is a specific number, e.g. 213,432,237,905,197.

1.6.2 Grover's Algorithm

Complementing Shor's algorithm[57], the Grover search[76]algorithm affects the security of algorithms based on symmetric cryptography. It provides significant speedup for many problems, such as optimisation and factoring large numbers into a product of two prime numbers. Classically these types of problems are resolved using brute force search.

AES is considered a secure algorithm for IoT-based communication. The algorithm is based on utilizing a single key for encryption and decryption. Brute force is the most recent attack on the security of AES cryptosystems. It executes by covering all possible keys. The complexity of the brute force attack is 2^n if the size of the key is n bits[55]. Therefore, until approximately 2030, by considering Non-Quantum compute availability, a minimum of 112–bit security is considered safe. The famous Grover[49] algorithm speeds up the process of brute force attack. Hence, we need 256 bits of the key to achieve the same level of security as the 128-bit key. The futuristic scenario is that a 128-bit key will offer roughly the same level of security as a 64-bit key today whenever the Quantum computer is available[73].

1.7 Quantum Cryptography

Quantum Cryptography exploits Quantum mechanics to perform cryptography[77]. To interrupt the security of Quantum cryptography-based schemes, one should violate the Quantum physics laws, which are unworkable. Hence, Quantum Cryptography offers robust solutions to counter traditional security threats and Quantum attacks on established cryptographic systems. To achieve high-security framework, Quantum Key Distribution(QKD) and Greenberger-Horne-Zeilinger states (GHZ) states are discussed as:

1.7.1 Quantum Key Distribution

The strength of the classical cryptography mechanism depends on the key distribution of secret key (symmetric) and public-key (asymmetric) cryptosystems. However, a problem with these is that the key transmission over an unreliable channel indicates that a third party may be on the communication path to intercept the key. Then adversaries use that secure key to decode secret user messages. Therefore, distributing keys without compromising the network's security is challenging. Quantum Key Distribution(QKD) provide solutions to the above-mentioned issues. The procedure is based on key distribution and not on message encryption. In QKD, two channels Quantum and classical, are used among communicating parties. The Quantum communication channel is used for secret key exchange. However, the classical way was used to demonstrate whether the shared key is distorted or not[78].

In this process, the photon polarization represents a particular state of a particle, which corresponds to each bit in a key. These bits are the foundation of Quantum Cryptography. The Quantum Cryptography is the principle of QKD[63]. In QKD, bits are transmitted using specific polarization angles. The two-bit values $|0>$ and $|1>$ are distinguished using polarization angle, also known as random basis. These bases are used each time to transfer keys securely. These two bases are more specifically referred to as rectilinear and diagonal basis. If we consider a rectilinear basis, photons are polarized at angles 0° or 90°. These photons, in turn, represent bit values 0 or 1, respectively. However, if the basis is diagonal, photons polarized at angle 45° represent bit 0°, and at angle 135°, it represents 1. Here, for ease of simplicity, these specific angles 0°, 90°, 45° and 135° can be written as H and V for horizontal and vertical. The D and A are used for diagonal and alternate. In polarization basis, the basis H, V is further denoted by + and D, A by X[79]as represented in Table 1.9.

Table 1.9: QKD random basis and its representation

Basis	Bit value		Notation		Basis Representation
	0	1	0	1	
Rectilinear	0°	90°	H	V	+
Diagonal	45°	135°	D	A	X

However, the popularity of these conventions can be seen in the BB84 Protocol[57], categorized as the QKD protocol.

1.7.2 Greenberger-Horne-Zeilinger

An analysis made by Greenberger, Horne, and Zeilinger in 1989 on the entanglement of more than two particles comes out as Greenberger-Horne-Zeilinger states (GHZ) states[80]. The GHZ states that tracing out only one entity destroys entanglement in the state. The state ends up in a fully mixed state. These GHZ states maximize entanglement particles and are therefore referred to as maximally entangled states as in Eq1.14.

$$|GHZ >= \frac{|0 >^{\otimes n} + |1 >^{\otimes n}}{\sqrt{2}}, n > 2 \tag{1.14}$$

Eq1.14: represents the n-qubits GHZ states shared among n number of entities. In our proposed protocol, the correlation among three communicating parties sharing the GHZ states can be expressed as in Eq.1.15:

$$|\Psi >_{GHZ}= \frac{1}{\sqrt{2}}(|0 > |0 > |0\rangle + |1 > |1 > |1 >) \tag{1.15}$$

These GHZ states could be created by legitimate parties to obtain confidential information. It is also used to generate a secret Quantum key.

1.8 Motivation

IoT technology provides many benefits, but it also increases security threats. Classical Cryptography is not feasible when we want to secure IoT communication. The existing classical schemes are not designed to resist Quantum attacks. Quantum Computing has supreme processing power. Quantum Cryptography has attracted many researchers to provide Quantum-based solutions for future IoT communication. Therefore, there is a need to find Quantum-based IoT solutions for secure IoT communication. The Key motivation of our work is as follows:

1. Quantum Computing-based algorithms such as Shor's and Grover's algorithms have already proven that they can break the security of classical cryptographic primitives.

2. Quantum authentication schemes which enable legitimate entities to identify eavesdropping in the IoT communication environment need to be identified.

3. The data transfer scheme based on Quantum principles for a secure IoT communication framework must be implemented.

4. There is a strong need for novel Quantum secure key distribution and mutual authentication framework which covers both Classical and Quantum attacks.

1.9 Research Gaps

This section presents the research gaps identified from the existing literature.

1. One of the main issues with classical cryptography is establishing shared secret keys communicated over an insecure channel. Therefore, the main challenge is to find a method to securely distribute secret keys.

2. Most of the work done previously does not provide a mechanism for detecting the eavesdropping attack, which is essential for secure IoT communication.

3. Quantum Computing has an impact on mutual authentication protocols which were based on classical cryptography; hence Quantum, resistant authentication protocols are required for secure communications.

4. For a secure IoT communication environment, there is a need to adopt and develop algorithms that are able to resist Classical and Quantum attacks.

5. Further research is also needed to handle the challenges of developing more advanced algorithms to enable higher-quality data communication and longer transmission distances for Quantum Computing protocols.

1.10 Research Objectives

The aim of the thesis is to identify solutions for securing IoT communication frameworks from classical and futuristic Quantum attacks. This objective can be achieved on several levels as follows:

1. To conduct a systematic literature survey on cyber-security issues and Quantum-based solutions for improving the security of IoT communications.

2. To design a mutual authentication scheme based on Quantum Cryptography.

3. To design a Quantum-Based cryptosystem for secure data transmission by considering major attacks against IoT applications.

4. To analyze the performance of the Quantum schemes in the resource-constrained IoT network.

1.11 Contributions

The main contributions towards this thesis have been summarized in the following subsections.

1. **QAKA: A Novel Quantum Authentication and Key Agreement (QAKA) protocol using Quantum Entanglement for Secure Communication among IoT Devices**

   This work presents a novel Quantum Authentication and Key Agreement (QAKA) protocol based on GHZ states and QKD protocol to achieve a secure framework[81] is presented. The GHZ states can be used to create maximally entangled three-particle states. These states are generated by splitting Quantum information into two parts. Due to the characteristic of the maximally entangled photon, the complete particle is required to reconstruct the original qubit. The secret key is essential within a communication network. the proposed protocol ensures a secure Key Agreement (KA) and Mutual Authentication (MA) based on Quantum hashing with Quantum Passwords(QP) and Quantum Teleportation method. The implementation of

Quantum GHZ states for the proposed protocol on IBM Quantum Experience is presented. Formal security analysis of the scheme, including the simulation using the widely-accepted AVISPA tool with BAN and ROM shows that the scheme is secure against various known attacks. Informal security analysis of the proposed scheme ensures the security proof of the proposed scheme. The performance analysis of the proposed protocol is compared with other IoT authentication protocols.

2. **QSMAH: A novel Quantum-based Secure Cryptosystem using Mutual Authentication for Healthcare in the Internet of Things**

   This work proposes a novel Quantum-based Secure Cryptosystem based on Quantum Cryptography. The QSMAH protocol utilizes GHZ states to ensure authentication between the Patient and MP before secret communication occurs. The data is transferred secretly from patient BSN to MP using a Quantum Key Distribution (QKD) scheme. Quantum Key requires each entity to participate equally in the key generation process. We have implemented the Quantum circuits on IBM Quantum Experience (IQE) for the proposed protocol. To prove the goal of our protocol, an extensive formal security analysis using BAN logic is provided. The proposed protocol is simulated using Automated Validation of Internet Security Protocols and Applications (AVISPA). The proposed protocol ensures the security of patients' data from both classical and futuristic Quantum attacks.

1.12 Outline of the Thesis

The organization of this thesis is as follows.

Chapter 1 gives a brief overview of IoT security issues and Quantum impact on existing Cryptographic schemes and discusses the objective behind our research work on Quantum cryptography for IoT security.

Chapter 2 presents the existing related work for authentication in IoT and some practical preliminaries used in our work.

Chapter 3 Quantum Authentication and Key Agreement (QAKA) protocol for securing IoT communication framework is presented. Additionally, we demonstrate that our scheme provides better efficiency and security when compared with some related schemes.

Chapter 4 Quantum-based Secure Cryptosystem using Mutual Authentication for IoT-based Healthcare(QSMAH) is presented. Besides, we prove that the proposed scheme is resistant to both Classical and Quantum attacks.

Chapter 5 presents the comparative analysis of the proposed schemes with existing authentication schemes.

Chapter 6 summarizes the thesis by highlighting the contributions, and it also discusses some future research directions.

Chapter 2

LITERATURE REVIEW AND PRELIMINARIES

2.1 Introduction

In this section, we analyze some of the classical authentication schemes from the security point of view. However, we have identified several flaws in each of the schemes. Most existing schemes focus on symmetric and asymmetric cryptography for Key distribution and authentication. We analyzed the Quantum Cryptography and Post Quantum schemes for secure IoT communication. We also presented a comparison between classical Quantum schemes.

2.2 Quantum Computing for Secure Internet of Things

The usage of IoT is expanding in many applications, such as intelligent environments, cities, smart grids, etc. The number of devices connected in IoT communication provides decision-making ability to users. This vast spectrum of IoT-enabled applications[82], as represented in Figure:2.1, transfers a massive amount of data, which imposes security and privacy challenges. Without authentication and privacy, IoT applications will not be able to reach high demand. It may also create serious security threats to their potential users. IoT has challenges such as privacy, confidentiality and authentication. The existing scenario of IoT applications is based on RSA and ECC-based schemes[26]. However, with the emergence of Quantum Computer, such encryption primitives will no longer be secure. Quantum computer solves these classically unsolvable problems based on classical cryptographic primitives. Therefore, the security of this IoT communication network is ensured by Quantum Computing. Quantum Computing is based on the principle of uncertainty [59] and the no-cloning theorem [83]. The main aim of studying Quantum Computing is to design protocols and algorithms to resolve IoT security issues, which are Quantum-resistant. Classical computing manipulates individual bits, whereas Quantum computer uses qubits. These qubits, with their associated probability, represent the Quantum state. These qubits are based on Quantum mechanics principles such as superposition and entanglement. Superposition allows qubits to be in different possible combinations of values simultaneously. Entanglement creates a strong dependent relation between Quantum particles. However, with the advancement of Quantum Computing, the existing encryption methods are at a significant threat.

Quantum key distribution(QKD) [61] is a highly active research area in Quantum Computing.The foundation of the Quantum key depends on Quantum mechanics [82]. It enables communicating parties to establish secret keys to communicate securely. Quantum Computing provides many benefits to the futuristic world, such as creating life-saving

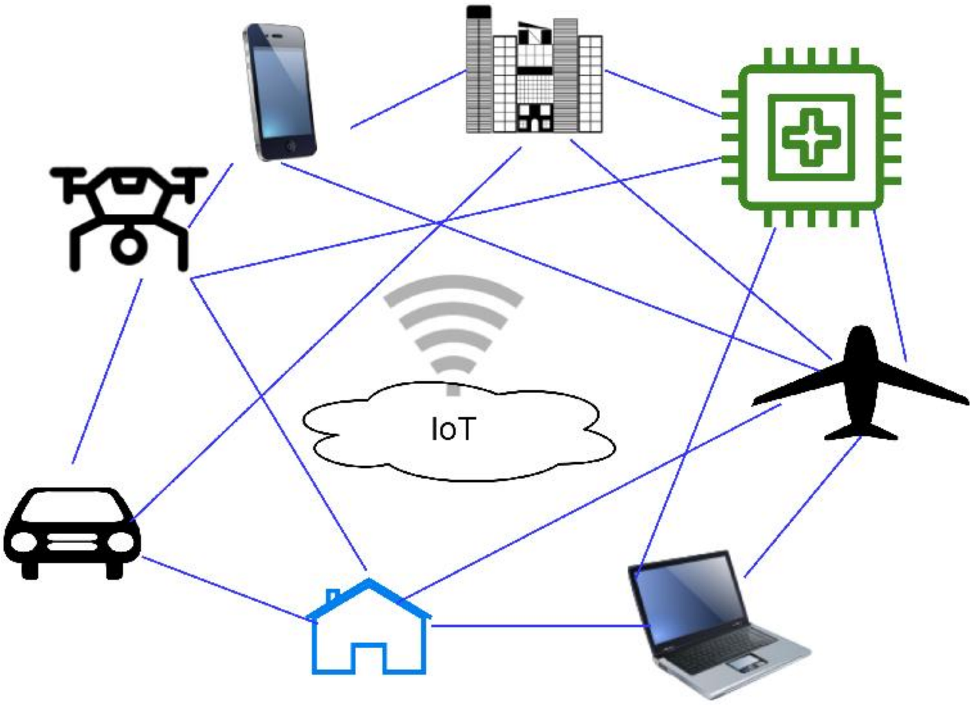


Figure 2.1: Futuristic IoT architecture

medicines, advancing artificial intelligence, and creating intelligent infrastructure. The recent advancements in Quantum Computing impose threats to cyber security algorithms. In the literature, many advantages of Quantum Computing for securing IoT communication based on the BB84 protocol have already been proposed. Many branches of Quantum Computing for secure IoT communication, such as QKD[84], Quantum entanglement [85], and Quantum Walk(QW) protocols[86], have already been explored in the existing literature.

The basic building block of Quantum Computing is shown in Figure:2.2, consisting of Quantum physical building blocks, Quantum Logic gates and a Quantum programming environment.

2.2.1 Quantum-based Layered Architecture for IoT

IoT framework is an interconnection of heterogeneous devices interconnected with diverse technologies such as Wifi, Bluetooth, Zigbee, Bluetooth, and 6LOWPAN. These are IoT-enabling technologies. These technologies enable data transfer in IoT applications such as smart cities, innovative medical infrastructure and intelligent farming. These applications require data privacy and confidentiality; therefore, IoT integration with Quantum Computing plays a significant role. In addition to that, the need to handle classical and Quantum attacks opens the door toward Quantum-cryptography[87].

We also reviewed the benefits of integrating the Quantum-based layer into the existing IoT layer architecture and its future perspective as represented in Figure2.3.

2.2.1.1 Sensing Layer

This layer enables various sensing technologies, such as WSN, RFID, and GPS, which deal with IoT sensors and actuators. Various sensors for perceiving data from surroundings,

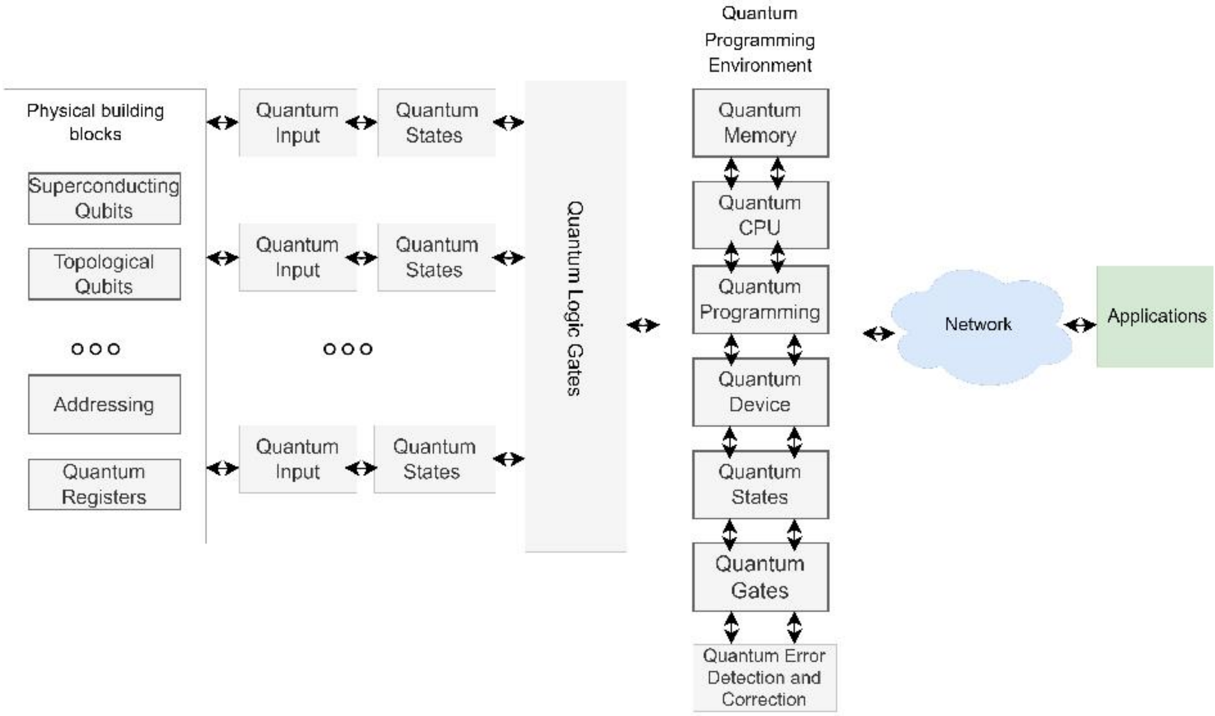


Figure 2.2: Architecture of Quantum Computing

such as ultrasonic, camera, and temperature detection, are used. Various attacks on this sensing layer are possible, such as sensor node capturing, false data code injection, eavesdropping, and sleep deprivation attacks.

2.2.1.2 Network Layer

Computational units must process the data received from the lower (sensor) layer. The network layer's function is to send the information acquired from the sensor layer to processing units. The processed data is required to enable IoT applications. However, due to open internet connectivity, network layers face serious security threats, such as access control attacks, DoS attacks, attacks during data transients, etc.

2.2.1.3 Quantum Layer

The Quantum layer provides security to IoT applications. It includes secure key distribution. Due to Quantum mechanics laws, the privacy and security of keys are guaranteed at this layer. However, this layer enabled Quantum- based cryptography, which will suffer from security threats such as individual, collective and coherent attacks.

2.2.1.4 Application Layer

The application layer is accountable for providing services to the user for decision-making. Critical IoT applications are smart cities, intelligent environments, competent health care, and intelligent grids. IoT heterogeneous applications have severe issues of privacy, confidentiality, and data authentication. Eavesdropping attacks, access control, service interruption attacks, and malicious code attacks are the major issues at the application layer.

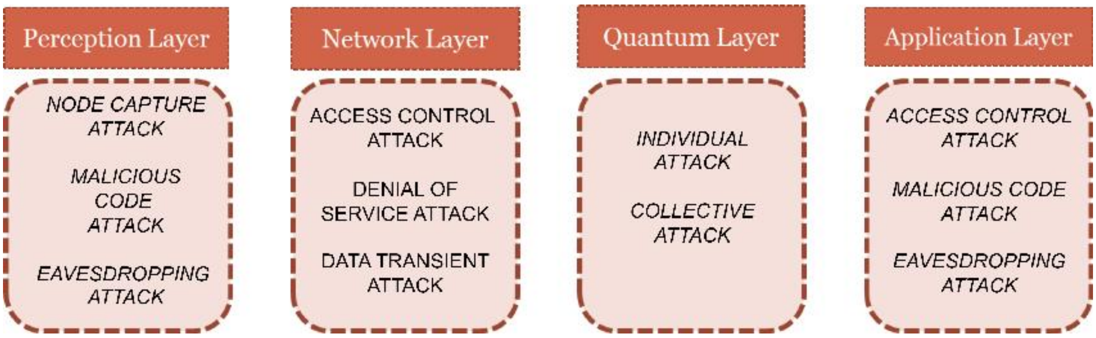


Figure 2.3: Security threats on IoT layer architecture.

2.3 Classical Cryptography to Quantum Cryptography

The future IoT idea is that the Internet's global, dynamic living structure would be available, sensed, and interconnected. WSN play the foremost role in IoT communication. The sensor node transmits messages to the user device via the GWN. The data transmission is done between these communicating entities through an insecure network. The messages exchanged using insecure communication channels can be intercepted, modified, or re-routed by an attacker/adversary[88].The IoT devices are vulnerable to attacks such as man-in–middle, impersonation, replay, gateway node bypassing and DDoS attacks. Such devices need mutual authentication to verify their counterparts. The discussions regarding application-specific mutual authentication protocols have dominated research in recent years [89][90]. Most widely accepted classical cryptographic techniques, such as RSA, rely on popular asymmetric cryptosystems[70]. The security of RSA is based on the prime factorization method. Once Quantum Computing algorithms[90] are available, they threaten the security of most classical algorithms based on symmetric and asymmetric cryptography. The Quantum Computing-based Shor's algorithm[73] shows concerns about the security of the prime factorization-based cryptographic algorithm.

In prior research, various authentication techniques[91] have been proposed for safe communication.Later, it was found that all those techniques were vulnerable to security attacks launched by Quantum Computer[92]. Quantum computers have exponential power in computation because of Qubits. In our work, we analyzed that hackers are storing a lot of data they can decrypt later by using Quantum Computer. Therefore, we analyze the roadmap from classical to Quantum resistant schemes by understanding 5G-enabled IoT security concerns and limitations of classical cryptosystems. It is considered the most urgent requirement to prepare for Quantum-based algorithms that can also withstand classical computer attacks. Furthermore, in IoT communication, it is a complex task to secure a secret key and verify authorized users. Therefore, key management and authentication are the major research issues. As illustrated in Figure 2.4, critical concerns such as key management, user access control, device authentication, and intrusion detection must be addressed to ensure secure communication within IoT [93]. Some authors proposed security protocols for different categories of key management issues such as "device authentication" and "User authentication" [94, 27].They also consider"intrusion detection" and "user access control".

The cyber-attacks identified in 5G IoT-enabled communication greatly impacted user privacy, identity authentication, and consequential security risks[95] to its powered de-

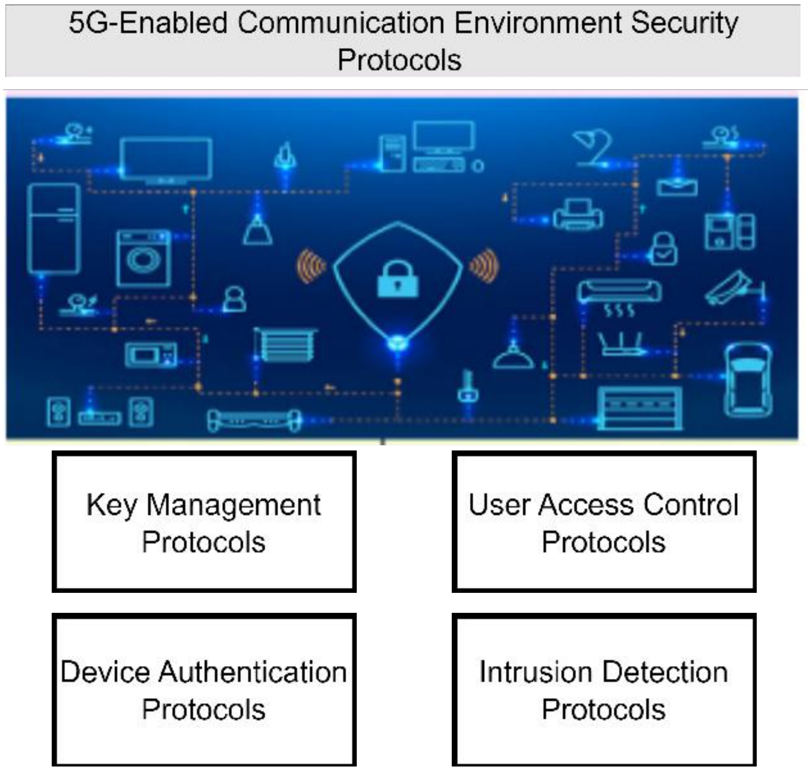

5G-Enabled Communication Environment Security Protocols
Key Management Protocols
User Access Control Protocols
Device Authentication Protocols
Intrusion Detection Protocols

Figure 2.4: Significant development in Quantum Computing theories [A-Inventor; B-Significant contribution.

vices. In an IoT environment, a key management scheme uses a cryptographic approach that keeps the records of trusted users and different smart devices involved. Table 2.1 shows the protocols for key management and authentication examined by various researchers.

Table 2.1: Existing key agreement and authentication protocols for 5G-enabled IoT

Author	**Authentication Protocol**	**Resilience against Attacks**	**Key areas covered**	**ASVT**	**Privacy**	**Protection**	
					A	**I**	**C**
Seok et al.[96]	Lightweight Authentication Protocol With associated data (AEAD) Ciphers	Impersonation, Eavesdropping, Privacy,sensor node sniffing.	Covered Resource-Constrained IoT devices.	-	✓	✓	✓
Sharma et al.[97]	Authentication framework assisting user privacy-preserving and key authentication.	Attacks on confidentiality, Integrity and Availability	5G threats due to public access connectivity.	Scyther	✓	✓	✓
Basin et al.[98]	5G AKA protocol.	Location attacks, replay attacks	Mutually authenticating subscribers and their carriers and establishing a secure channel to protect subsequent communication.	Tamarin	✓	✓	✓
Gong et al.[99]	Mobile edge computing architecture.	Denial of Service(DoS)	-Secondary and data management authentication functions	-	✓	×	×
Chaudhary et al.[14]	Authenticated mobile devices Kerberos in the 5G communication framework.	Distributed Denial of Service (DDoS).	Authentication considers kerberos as a solution for attacks such as DDoS.	Python	✓	×	×

A-Authentication, I-Integrity, C-Confidentiality, ASVT-Automated Security Verification Tool

Moreover, the key management protocol generates, distributes, establishes and manages cryptographic keys to differentiate between malicious and legitimate entities[93].5G-enabled IoT attacks are not limited to domain name system (DNS) attacks[8], password guessing and cracking. Future attacks are more descriptive and vulnerable, which can be categorized based on three cryptological parameters:

(a) **Mutual Authentication** -In a 5G-enabled IoT, authentication is highly important as it involves both parties authenticating each other. Authentication between smart IoT devices is important to protect the network from Sybil, impersonation, identity-based attacks, etc.

(b) **Confidentiality** - Cyber-attacks are flourishing in digital communication; hence, hiding information from attackers like user private data and security keys is required. In the realm of IoT, 5G facilitates communication, but it also exposes vulnerabilities to passive attacks like packet sniffing and phishing, which can compromise user's sensitive data.

(c) **Integrity**- In a communication network, adversaries could access, monitor, and access authorized users' service requests. Additionally, this unauthorized person could also capture user credentials and user equipment. Integrity assures real and accurate data. It ensures user received data is not modified, deleted or illegally injected. An attacker may attack integrity by introducing session hijacking attacks, Man–In-Middle, etc.[100].

2.3.1 Classical Schemes

This section also discusses various Security Consideration(SC) on IoT and possible traditional countermeasures[101]:

1. **Safe Against Impersonation(SC1)**
   Considering a scenario, adversaries share user information with the gateway. The adversary tries to ensure GWN that the message is coming from an authenticated user by forging user credentials. This attack is also caused by flooding the system by spoofing. However, it can be detected by acknowledging each request and maintaining its sequence number[96].

2. **Gateway node bypassing (SC2)**
   This attack considers a scenario when an attacker directly accesses data shared by sensor nodes without participating in the gateway node. Authentication of gateway nodes is required to maintain data integrity[91].

3. **Privacy sniffing (SC3)**
   In 5G-enabled IoT communication, it is considered a potential attack in that an attacker can launch further attacks. The eavesdropper exchanged messages between communicating parties, sensor and sniffed email traffic, router configuration, and chat sessions[93].

4. **Replay attack(SC4)**
   In this type, the attacker seizes the data shared between communicating entities and repeats the message to extract secret information. Additionally, an attacker can deceitfully delay or retransmit the message to confound the receiving entity evaluating it. In the 5G IoT scenario, one-time passwords, nonce, time stamps, and

Media Access Control (MAC) are to be created for mutual authentication to prevent such an attack.

5. **Gateway Forgery (SC5)**
   An attacker tries to acquire transmitted messages from GWN. The authenticated gateway node is required to prevent such an attack[91].

6. **Location Spoofing (SC6)**
   Such an attack occurs in the communication environment when devices are communicating with each other. An attacker may broadcast a request message with the wrong location information to disrupt communication. Therefore, device validation is required for messages' authenticity [101].

7. **Man-In middle (SC7)**
   In this, the attacker intercepts network data to gain unauthorized access. The attacker expropriates the transmitted messages, making users believe they are talking directly but infecting the conversation.

8. **Denial of Service (SC8)**
   DoS can be explained by considering a scenario where an attacker floods the target with traffic to capture and completely deplete memory resources. Additionally, it disallows legitimate users' access to resources due to this enormous traffic[96].

9. **Privileged-insider (SC9)**
   An attacker may be a privileged insider or trusted authority who can exploit stored information to unauthorized parties. In addition, session key computation and password guessing attacks[93].

10. **Traffic Analysis(SC10)**
    This attacker listens to network communication to determine application behaviour patterns, routing structure, location of key nodes, and base station location [93].

11. **Mutual Authentication (SC11)**
    The entities must register themselves before any communication process starts. The authentication ensures that two authenticated parties communicate with each other, reducing the probability of non-repudiation and user impersonation attacks. Authentication between the communicating entities must provide safe communication.

By considering the attacks on IoT communication such as eavesdropping and impersonation,etc. Several classical security solutions explored by researchers as represented in Table2.2, as these countermeasures are based on symmetric and asymmetric keys detailed descriptions provided as:

(a) **Public key Authentication:** Asymmetric-cryptosystem relies on the mathematical formulation of problems based on the prime number and discrete logarithm. In this process, secret messages are exchanged between sender and receiver through the internet[102]. The only people who can get meaningful information from the message are the authenticated users with private keys. Moreover, authentication protocols rely heavily on finding the private key from its paired public key. The computing capabilities of private and public key pairs should be kept computationally efficient, especially for deploying wireless IoT[103]. These schemes require further analysis to provide lightweight and computationally logical privacy preservation.

(b) **Private Key authentication:** In authentication protocols based on symmetric cryptography, communicating parties share a common secret key for communication. In this method, both entities, i.e. sender and receiver, have the private key for secretly communicating. For instance, the AES, DES and their variants Double DES and Triple DES provide secure communication between sender and receiver[104]. Avoine et al.[105] proposed a three-party secure key interchange protocol based on the private key concept. Their protocol considers a realistic IoT deployment that involves numerous end devices and servers.

(c) **Hashing:** The hashing technique inputs variable-length messages and produces fixed-length code by applying mathematical operations. Due to the massive D2D, H2M and M2M connectivity, user passwords are prone to security attacks. Therefore, hash-based schemes are required to protect passwords. The key agreement's digital signature method and random sequence generators are a few examples of hash-authentication-based cryptographic applications[55]. Turkanovic et al.[106] proposed a mutual authentication scheme based on establishing a shared cryptographic key between the sensor node and the user outside the network. In their scheme, these authors use only simple hash and XOR computations and adapt to the resource-constrained architecture of the WSN.

Table 2.2: Techniques adapted by existing authors in the present IoT scenario and their weaknesses

Author and Year	**Security threats**	**Techniques**	**Advantages**	**Weaknesses**
Lu et al. [107] 2019	-Impersonation -Privacy Sensor node -sniffing	Elliptic Curve Cryptography(ECC)	Less memory and computation cost	Data integrity and authentication
Wu et al. [108] 2016	-Gateway node bypassing attack -Replay attack	- Hash Function - XOR computations	- Resilient against the secure key agreement, authentication, credential updation, protection and user anonymity.	Network attacks are possible.
Althobaiti et al.[11] 2013	Attacks: - Eavesdropping -Insider -Gateway forgery attack	-Biometric encryption - Hash Function	- Suitable for both Homogenous and heterogeneous environments.	Mutual authentication and confidentiality of data.
Gope et al.[109] 2018	-Location spoofing	-Lightweight RFID-based authentication.	- Easy tracking of real-time objects. - Low cost	Impersonation attack. Limited computing and storage capabilities of RFID Tags.
Deng et al.[110] 2014	-Traffic analysis	- Anti-traffic analysis strategy - Differential Fractal Propagation (DFP) Algorithm -Multi-parent routing scheme -Random walk	-Low overhead and energy consumption.	Time correlation attacks.

Many researchers proposed user authentication schemes for secure IoT communication. These schemes are one[111, 112], two[35, 36, 37, 38] and three-factor[48, 40] authentication schemes. We discuss two and three-factor schemes in this section. One parameter is based on knowledge factors like passwords, but it is not considered secure due to heterogeneous and resource-constrained 5G-ad hoc wireless sensor networks.

2.3.1.1 Two-Factor Authentication Schemes

The 2PAS uses two parameters for authentication: entity password, biometric data, and an E-Smart card. Watro et al.[99] use two parameters in their scheme password and smart card for authentication. The cryptography algorithms used in their work are RSA and Diffie Hellman. They worked on a lightweight sensor node to implement a public-key-based protocol called TinyPk. The weakness of their scheme is that they do not safeguard against user masquerading attacks, as reported in[100][37] provided a secure network communication considering stolen-verifier attacks based on the hash function. Table 2.3 outlines the security aspects addressed by various authors.

Table 2.3: Security Considerations by Researchers Based on Two-factor Authentication

Authors	SC1	SC2	SC3	SC4	SC5	SC6	SC7	SC8	SC9	SC10	SC11
[100]	–	–	–	✓	–	–	–	–	–	✓	–
[113]	–	–	✓	✓	–	–	–	✓	–	–	–
[114]	✓	–	✓	–	–	–	–	–	✓	–	–
[115]	✓	–	–	–	–	–	–	–	✓	–	✓
[88]	✓	–	✓	–	–	–	–	–	✓	–	✓
[116]	–	–	✓	✓	–	–	–	–	–	✓	–
[117]	✓	–	✓	–	–	–	–	–	✓	–	✓
[118]	✓	✓	✓	✓	–	–	–	–	✓	–	✓
[119]	✓	–	✓	✓	✓	–	–	–	✓	–	✓
[114]	✓	–	✓	✓	✓	✓	–	–	✓	–	–

2.3.1.2 Three-Factor Authentication Schemes

The Two-factor communication protocols are secured until and unless passwords or smart cards are stolen[91]. Table 2.4 shows the security breaches examined by various authors in their respective research contributions.

Table 2.4: Security consideration of Three-Factor authentication schemes.

Authors	SC1	SC2	SC3	SC4	SC5	SC6	SC7	SC8	SC9	SC10	SC11
[113]	✓	–	–	–	–	–	✓	–	–	–	✓
[11]	–	–	✓	✓	–	–	✓	✓	–	–	✓
[107]	✓	–	–	✓	–	–	–	–	✓	–	✓
[114]	✓	–	✓	✓	✓	–	–	–	✓	–	✓
[120]	✓	–	✓	✓	✓	–	–	–	✓	–	✓
[116]	✓	–	–	–	–	–	–	–	–	–	✓
[121]	✓	✓	–	✓	–	–	–	–	✓	✓	✓
[122]	✓	–	–	–	–	–	✓	–	✓	–	✓
[116]	✓	–	–	–	–	–	✓	–	–	–	✓
[113]	✓	✓	–	✓	–	–	–	–	✓	✓	✓

✓Provided countermeasure against Security consideration; – Not covering the security consideration

Whilst 3PAS strengthens the security more than 2PAS. The added third parameter, biometric identification, makes it difficult for an eavesdropper to tamper the security. Chang et al.[120] proposed an authentication scheme based on key agreement. They aim to resolve weaknesses of 2PAS, such as lost E-Smart cards and impersonation attacks. However, later Jung et al.[121]reported that[120] it does not safeguard against impersonation and credential guessing attacks. Chang et al.[116]analyzed that[106]is vulnerable to user impersonation, node capture and spoofing attacks.

2.3.2 Quantum based Schemes

The authentication schemes discussed above, proposed by many researchers, are based on two and three parameters. The recent practical implementation of these schemes proved that these are not secure under many classical and futuristic Quantum attacks. The main loopholes and challenges may be summarized as follows:

1. **Something you know: Passwords or Pin**
   No security is infallible. The user credentials that provide two-factor authentication are saved in an E-smart card. Although the 2FAS scheme is more successful and powerful than a single factor, it is still inefficient. An adversary can easily get a user's personal information through fake websites by guessing passwords. In addition, they could also steal a user's phone from which they can access SMS and email information.

2. **Something you have: Security Token or Smart Card**
   For security, smart cards have been widely used for authentication purposes. The smart card is a proximity tag. These are used for many purposes, such as building access, identity confirmation, etc. Each card has a specific ID that differentiates it from others on the network. This identity is further passed on to the reader. Whenever any user accesses the system, this unique ID confirms their identity. Based on which their access is granted or denied. However there are huge benefits of smart cards, but the overall estimated cost is between 75 and 100 dollars for implementing these E-smart cards and their subordinate devices. Suppose a company has thousands of customers or employees. For this, the implementation cost of smart cards could reach millions. Due to their small size, these smart cards are often lost and can be used by an unauthorized person.

3. **Something you are: Biometrics**
   The authentication schemes based on biometrics provide more cost-effective solutions than OTP or token-based schemes. In biometrics, physical characteristics such as fingerprints, retinal data, or even facial features provide authentication if performed under controlled circumstances (e.g. guarded). However, it has been analyzed that these biometric identity-based features are difficult to spoof. However, it is not feasible as this data may easily be replicated. The entire biometric information will become meaningless if there are security breaches. However, considering the storage of biometric data could also be difficult as it raises the security implications of a data leak. The solution to the abovementioned problem is called cancellable biometrics to preserve user privacy. Cancellable biometrics is implemented using 1) Biometric Salting and 2) Noninvertible Transforms [122]. However, this solution has certain limitations in that it will only work under certain situations, such as when the client biometric data exact copy is available to the server.

4. **Implementing Authentication Schemes: Time-Consuming**
   Time may be a perfect metric, but it's also relative. The time lost in implementing 2PAS depends upon what form an organization adopts. For example, SMS-based 4-digit privacy codes are faster to navigate than others. The authentication schemes under 2FA increase the time to access accounts. It does that by adding a new factor to the authentication. Now, if we are considering each entity level, this would be minuscule. However, organizations with numerous employees add up to thousands of work hours lost yearly in implementing this scheme.

5. **Error Tolerance and Nontrusted Devices**
   The biometric data collection process is prone to various noises. Due to noise, it's impossible to reproduce biometric information as measured precisely. One issue with practical biometric authentication protocol is the comparison of the encryption of biometric templates. These protocols required an exact match. Another issue in biometric authentication is that the server should perform only biometrics verification instead of verifying any user devices. Such devices cannot be fully trusted due to their distance from the server.

6. **Heterogeneity: WSNs**
   Heterogeneity is a congenital feature of mobile computing. Mobile devices, wireless networks and the cloud are the three different categories of mobile computing. Heterogeneity preserves the connectivity of mobile devices. However, in mobile computing, the main security concerns are during handover. So, while designing authentication schemes, the diversity of framework, technologies, hardware, infrastructure, and handover mechanisms must be considered.

7. **Failure can be disruptive**
   In authentication schemes, the more factors you add, the more successfully we can prevent unauthorized access and increase complexity. However, these factors add more complexity to the systems but may also create hurdles for an attacker. The attacker would have to jump through many factors to gain access. Moreover, integrating IoT with different objects creates various issues in people's daily lives, and delivering robust security to the IoT is challenging during transmission. Even the lightweight and privacy-preserving two or three-factor algorithm was provided. Still, the major problems and the possible attacks such as node capture, routing threats, impersonation attacks, brute-force attacks, message-tampering attacks and replay attacks are possible. Therefore, more security is required for secure network communication for future IoT environments.

From the above discussion, we identified that there is an urgency to develop security protocols to safeguard the IoT environment. Therefore, we reviewed the Quantum solutions to safeguard IoT communication in the next sections. From the above discussion, we identified an urgency to develop Quantum-Cryptography-based security protocols that can resist various classical and Quantum attacks.

2.3.2.1 Quantum Key Distribution

The secure protocol that two parties can use to exchange keys securely over a public channel is Quantum Key Distribution (QKD). The idea was based on Wisner's conjugate coding, later extended by Bennett[123]. The protocol achieves security by encoding information in Quantum states of light. The QKD protocols are sorted based on the Uncertainty Principle (prepare-and-measure-based), including BB84, B92, SSP, SARG04, and S13. However, others, such as E91, BBM92, DPS and COW, are Entanglement-based QKD protocols.

2.3.2.2 Uncertainty Principle-based Quantum Key Distribution

The protocol was published in 1984 and named by Bennett and Brassard[59], who implemented this first. Nine QKD protocols have been proposed, out of which five are based on prepare-and-measure(uncertainty)[57], while the other four QKD protocols are based on entanglement[124], as:

(a) BB84 Protocol
Preliminaries
Both parties must compute the total number of photons needed to form the secure key in advance. These numbers are used to identify the message's length. The BB84 protocol aims to deliver uninterrupted communication between sender and receiver by applying Quantum-computing notation (Bra-Ket). The BB84 protocol's four polarization states are represented in Table 2.5. The communication parties must agree that both:

1. Both parties must agree to share a sequence of randomly chosen photons based on one of the possible orientations: Rectilinear (0° or 90°) and Diagonal (45° or 135°).

2. No secret communication or information is exchanged over the network rather than key exchange.

3. As the final key is the product of both communicating parties, no one can individually determine the key in advance.

Assuming Alice (Sender) and Bob (Receiver) want to communicate with each other and Eve wants to intercept the basic message steps of the BB84 protocol as explained below:

1. Alice prepares photons (qubits) randomly chosen in polarization such as rectilinear 0° or 90° or diagonal polarization 45° and 135°. Before sending it to Bob, it keeps records of the polarization of each photon.

2. The users can interchange faint flashes of polarized light[63] represented by a rectilinear and diagonal basis. The basis is shared between those users who have not shared secret information.

3. The photons travel to a Bob. Then, for each photon, Bob considers a random basis.

4. The horizontal/vertical or diagonal polarization is used by Bob to "read" the polarization angle of each particle sent by Alice.

5. Bob keeps the log of the used basis and the resulting polarization measured.

6. Bob does not know each photon's horizontal/vertical and diagonal beam splitter. He can only make a guess.

7. If someone makes a wrong guess, he will get no information. For instance, if Bob analyses one photon with a diagonal filter sent by Alice using the rectilinear basis, then information about diagonally polarized photons is lost. Each measured photon selects one of the angles of polarization with a probability of 50%

8. After making random choices, only the basis is informed by Bob Alice. Actual results are not shared between Alice and Bob.

9. Bob will inform Alice only about the basis used to send measurement results.

10. Alice publicly informs Bob about the correct measurement results. Then Bob keeps a log of its accurate measurement outcomes.

11. The correctly measured bits create a one-time pad for sharing secret information. Both communicating parties discard the bits that do not match or are corrupted during transmission.

12. The accurately measured photons are then transformed into a string of bits based on polarization using a notation: $D = 0$, $A = 1$, $H = 0$ and $V = 1$.

13. QKD defines the procedure to generate the key by following this procedure securely.

14. The final key string consists of only those matched outcomes for which both the sender (Alice) and receiver (Bob) have the same measurement basis.

15. The string of bits generated in the final step of the key generation process contains numerous errors. These errors are due to many factors such as decoherence, noise in detectors, and Quantum channel disturbances. Additionally, during Quantum communication, other errors or disturbances might be created due to the presence of an eavesdropper.

16. Therefore, it is necessary to efficiently evaluate these errors to identify the adversary's presence in the Quantum communication channels. The Quantum bit error rate can be computed by comparing a small portion of the distributed Quantum key[74].

$$QBER = \frac{No.of Errors}{Total No.of Bits} * 100\%$$

Table 2.5: Representing polarization base of BB84 protocol

	Degree	Bra-Ket Notation	Basis(B1)	Degree	Notation	Basis(B2)	B1 and B2
Rectilinear	0°	$\|0>$	↔	90°	$\|1>$	↕	+
Diagonal	45°	$\|0>$	↙	90°	$\|1>$	↘	×

2.3.2.3 Entanglement-based Quantum Key Distribution

If two particles are entangled, measuring one attribute determines the state of the other. Figure 2.5 represents the entangled photon pair shared between two communicating entities. The photon pairs are exchanged using the Quantum channel; however, classical channels are used for sharing measurement basis. It also claimed that eavesdropping could be easily detected by evaluating results by considering Bell's inequality[124]. One

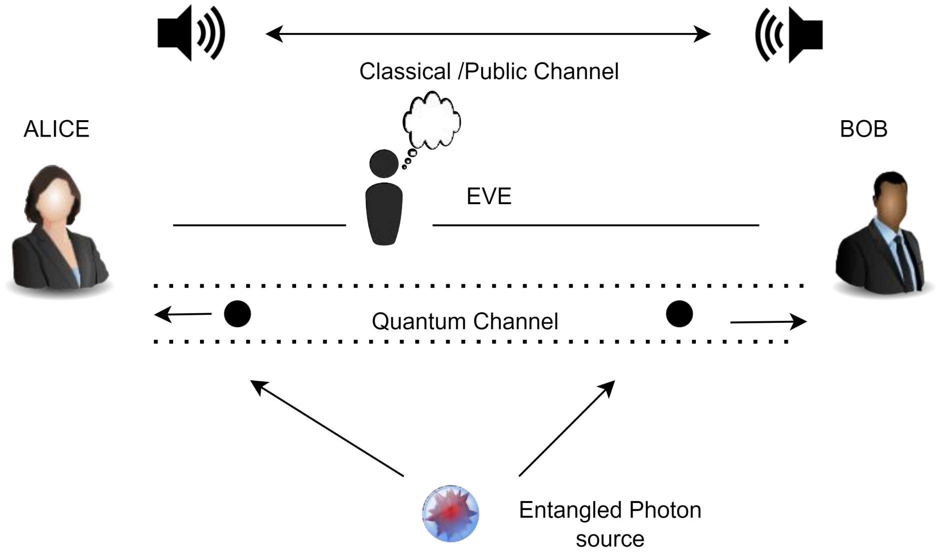


Figure 2.5: Entanglement-based QKD protocol

of the classic examples of entanglement-based protocols is E91, and there are some other entanglement protocols such as BBM92, DPS and COW[57, 124].

(a) **E91 protocol**- The protocol was designed using entangled pairs of photons. Ekert proposed the protocol in 1991[57]. Like BB84, chooses random measurement bases and utilizes the classical channel to identify the correct output string. The presence of an adversary on the Quantum channel could also be detected by computing the bell test.

(b) **BBM92**- This protocol was proposed by Bennett, Brassard, and Mermin[125] in 1992. The raw key exchange mechanism, key sifting, and privacy amplification are identical to BB84. It can be considered an entanglement-based version of BB84.

(c) **Differential-Phase-Shift (DPS)**- K.Inoue et al.[126]in their published work in 2003, they proposed entanglement-based QKD (DPS-QKD) named as DPS protocol. In comparison to the protocols above, DPS-QKD has a simple configuration. Moreover, the protocol is vigorous to photon number splitting (PNS) attacks.

(d) **Coherent One-Way protocol (COW)**- In 2004, Nicolas Gisin et al.[87] in their work consider time function for information encoding. Based on the concept of entanglement, the protocol has certain advantages. It provides high efficiency on distilled secret bits per qubit and tolerance to reduced interference visibility. COW protocol is also robust to photon number splitting (PNS) attacks like DPS.

2.3.2.4 Technical Challenges of Quantum Key Distribution

1. **Control and Organization of systems using Quantum Cryptography**
   QC provides huge security benefits to end-users. The limitation considers the end-user's control and organization of Quantum security protocols. The end-users cannot tailor the Quantum security services to fulfil their requirements. However, popular Quantum-based solutions allow customers to measure their particular security

requirements. The end-users then choose the right level of data protection[63] for their devices.

2. **Maximum Distance for Successful QKD transmission**
   Long distances Quantum communication is an important research issue. The challenge is due to the regeneration of the Quantum signal. The overall maximum distance covered by QKD transmissions[79] is over 200 km, successfully implemented. Additionally, the bit rate of QKD systems reaches only a few Mbit/s in a telecom metropolitan area network. Still, this disturbance is too high beyond 50 kilometres, which increases error rates. Therefore, it leaves the channel vulnerable to eavesdroppers and makes it virtually impossible to send information[74].

3. **Quantum Implementation Cost for high security**
   Until recently, only large companies, final institutions, and public administrations utilized the services of QKD techniques. Due to the huge cost involved in its implementation, QKD techniques are used by specific end-users [127]. However, the major cost incurred in implementing Quantum devices is the usage of optical fibre. These optical fibre links create a Quantum channel for transmitting Quantum bits.

4. **Quantum Entanglement-based Computing**
   Quantum entanglement is a method that can be very useful for detecting eavesdropping, but the cost associated with such a process is huge. However, considering the needs of the real world, keeping qubits entangled long enough is challenging.

5. **Different End-User Requirements**
   The level of security used by different platforms, such as E-financial services, public administration and large companies, varies greatly. It is complex to provide different end-user-specific services based on their changing demands. Users can only choose those services offered by network service providers. They can access the right level of data protection specific to their application. They cannot tailor these services according to their needs[74].

6. **Quantum Communication**
   In two-sided communication, the sender can always obtain more secret information about the receiver. However, the communication took almost ten years, but the fact mentioned above was noticed by Colbeck[128]. Similar work was done by Vein, Salvail, Schaffner and Sotakova[129].In this, the authors demonstrated that any Quantum information scheme can always leak to an unauthorized user. The worst scenario of any Quantum system is the leakage of information. This information leakage in any Quantum protocol is essentially as worst as one can assume. Moreover, considering probabilistic authorization and protection, one of the two communicating entities, sender or receiver, is considered secure.

7. **"Quantum rewinding": Zero-knowledge against Quantum adversaries**
   The zero-knowledge property is used in the classical world and is referred to as rewinding. The theoretical aspect of this is proved by implementing the given verifier. The verifier makes arbitrary choices that sometimes are not consistent with the desired outcomes. In this scenario, such computation paths are culled. This selection is based on tracing interactions. If the inappropriate path is followed, the entire computation is reset or rewind. A rewinding approach in the Quantum setting

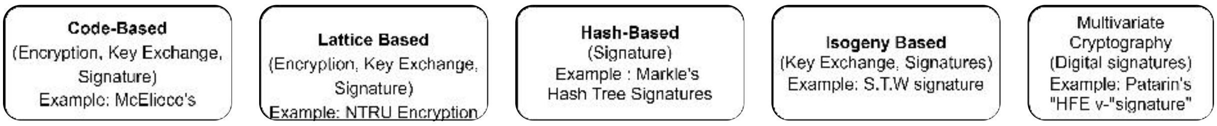

Code-Based
(Encryption, Key Exchange, Signature)
Example: McEliece's
Lattice Based
(Encryption, Key Exchange, Signature)
Example: NTRU Encryption
Hash-Based
(Signature)
Example : Markle's Hash Tree Signatures
Isogeny Based
(Key Exchange, Signatures)
Example: S.T.W signature
Multivariate Cryptography
(Digital signatures)
Example: Patarin's "HFE v-"signature"

Figure 2.6: An Overview of Post Quantum Family

is impossible. The system cannot maintain the alternative copy of the transcript or reproduce the state. Implementing and deploying Quantum rewinding in the context of zero-knowledge proofs is a complex cryptographic task that demands specialized cryptographic skills. IoT developers might encounter difficulties when integrating and managing these advanced cryptographic techniques.

8. **Quantum security notions: Superposition access to oracles**
   The security of classical schemes relies on mathematical cryptosystems. However, one can assume the Quantum adversary on such systems. Network security is often considered an interactive game between an adversary and a challenger. Therefore, to prove Post-Quantum resistance, the adversary can only win the game with zero probability. In this scenario, one must consider Quantum adversaries coordinating Quantum with the challenger. The chosen plaintext attack (CPA) learning phase is an example of a game-based security system. In this example, superposition is of plaintexts to be encrypted query by an attacker. The challenger then returned superposition-according ciphertext to the attacker. The superposition is for defining the indistinguishability (IND) security of encryption schemes.

9. **Position-based Quantum Cryptography**
   The main intention of position-based cryptography is to utilize the geographical position of an entity as a cryptographic credential. Consider the financial institution scenario, where the employee suffices as a credential to initiate the interchange of susceptible information. The main feature is the position verification of employees. The ultimate goal is to demonstrate the set of verifiers at a specific geographical location. Multiple attackers can break classical position-verification protocols. Classically, entities could easily simulate being at certain positions while their site is elsewhere. However, due to QM laws such as no-cloning on Quantum information, for collaborative attacks, one could come up with protocols that are impenetrable by these attacks, which later became insecure[129]. Integrating Position-based Quantum Cryptography into IoT systems could potentially lead to challenges related to managing devices, distributing cryptographic keys, and verifying their physical locations.

2.3.3 Post Quantum Cryptography

Recent attacks on IoT security frameworks necessitate changes in the existing cryptographic primitives. In this section, we discuss Post-Quantum Security Solutions(PQCS). These are code-based cryptography, secure signatures based on a hash function, multivariate polynomial cryptosystems, and Lattice-based cryptography, as depicted in Figure 2.6.

2.3.3.1 Code-based Cryptography

The Post-Quantum Cryptography scheme based on code structure is a candidate for Quantum-resistant schemes. It was proposed in the 1970s. It provides solutions to secure current cryptography [130]. The public key-cryptosystem [131] was proposed in 1978. It was the first proposed cryptosystem based on code. The entire[73] scheme was based on assuming the authentic platform for communication.McEliece cryptosystem is binary Goppa codes considered as the base of this scheme.Their scheme also adds an error purposefully to safeguard messages against adversaries.The input messages are encrypted using binary Goppa[7]. However, the overall security depends on the syndrome-decoding problem.It says that decoding is performed without any knowledge of the coding scheme.The LDPC (Low-Density Parity-Check) and MDPC (Moderate-Density Parity-Check) codes are other variants of the McEliece scheme.In code-based cryptography, the following steps are to be considered for generating cypher-text:

(a) The input data is added with random errors.

(b) By analyzing, forming a bit-error pattern by message encoding. The decoding recovers the original message by:

(c) Identifying and thereby eliminating mistakes from the input data.

(d) Removing the exact input message from the bit sequence of faulty codes.

It depends on the complexity of deciphering arbitrary linear codes, which positions it as a favourable option for safeguarding IoT devices from potential Quantum threats. One important aspect of a code-based scheme is hiding the code structure is of utmost importance. Therefore, an attacker with access to the specific code used for encryption would decrypt the message easily.

2.3.3.2 Lattice-based Cryptography

Lattice-based systems were formulated by Ajtai[55]. Lattice-based systems are formulated to solve problems such as the shortest vector in a high-dimensional lattice. A solution to these problems is computationally hard to find[125]. Göttert et al.[126]discussed and implemented in their work learning with errors (LWE) based cryptosystem. Lindner and Peikert propose these cryptosystems. Their scheme was based on matrix and polynomial-based variant comparisons of LWE. Boorghany et al.[132]in their work proposed lattice-based cryptographic Authenticated Key Exchange (AKE) protocols. Furthermore, the provably secure lattice-based cryptography is better than NTRU in running time. The discrete Gaussian sampling and FFT are secure lattice-based cryptographic systems[106]. Cao et al. [94] discussed a group of NB-IoT devices. These devices are for Quantum resistance access authentication and data distribution schemes. Their scheme considered lattice-based homomorphic cryptographic technology. Mitchell et al.[72]discussed the impact of future Quantum information computing on 5G-enabled mobile security. They also proposed a 5G-AKA protocol to overcome the drawbacks of classical cryptographic algorithms. Hence, lattice-cryptographic mechanisms also provide fast, Quantum-resistant solutions. These solutions were earlier assumed to be impossible to solve[55]. Lattice-based cryptography relies on mathematical challenges associated with lattice structures, which are considered complex for both classical and Quantum computers to address. It is considered a promising solution for securing IoT devices against the Quantum threat. Some of the authenticated protocols implemented by different authors, security issues and tools used to verify their model are represented in Table 2.6

Table 2.6: Lattice-based cryptographically secured authentication protocol

Authors and Ref.	**Authenticated Protocols**	**Security Issues**	**Verification Tool**
Cao et al.[94] and 2019	Lattice-Based Cryptography for NB-IoT	Signaling Congestion Avoidance Unlinkability, Protocol Attack Resistance	Scyther tool
Mitchell et al.[72]and 2020	5G-AKA	Mobile identity confidentiality,Session security	$--$
Boorghany et al.[133] and 2015	Authenticated key exchange (AKE) protocols	Confidentiality Authentication	JAVA, C++, ARM /THUMB compiler

2.3.3.3 Hash based Cryptography

These hash-based signatures are based on the one-time signature (OTS) scheme. The OTS scheme is based on a unique key pair [37]. The main flaw of this Quantum-resistant scheme is that two non-identical messages, such as a1 and a2, are signed using only one OTS key pair. In this case, by comparing these signed messages, the attacker can replicate this signature. An example is Merkle's hash tree based on the public-key signature system(1979)[134].Lamport gave the idea of Merkle's signature system, and [135] is based upon a one-message signature. In this binary, hash trees are used. The leaf nodes of the binary tree represent the OTS public key hash values. However, the parent nodes are calculated by concatenating the hashes of their child nodes. The parent node's authentication of the public keys of OTS is accomplished using the collision-resistance hash function[130], [133]. The hash-based signature scheme is in the process of standardization by the IETF[136], and it is referred to as the Extended Merkle Signature Scheme (XMSS)[7]. Hash-based signatures serve as a means to verify and protect communication integrity between IoT devices and gateways, guaranteeing that data shared among devices remains unaltered and resistant to interception.

2.3.3.4 Multivariate Polynomial-based Cryptography

There is almost no way to solve random multivariate polynomial systems. Therefore, they are categorized as NP-hard. Their dependency is on the utilization of multivariate polynomial systems. These systems are used to protect data collected by IoT sensors. In 1996, the technique of Patarin's Hidden Fields [55] –Public key signature system (1996) became popular based on the multivariate scheme. The proposed scheme was the generalization of the approach discussed by Matsumoto and Imai[55, 130, 7]. Several multi-variate cryptography schemes also exist based on Hidden Field Equations (HFE) trapdoor functions. These schemes are referred to as Unbalanced Oil and Vinegar encryption systems (UOV), Rainbow, and Tame Transformation Signature (TTS)[137]. The most popular signature scheme among these is HFEv due to its efficiency and ability to produce the shortest signatures among existing ones[73]. However, implementing a secure, robust and efficient multivariate cryptosystem scheme is an open challenge. Hence, many of those mentioned above multivariate public-key encryption schemes are not considered secure.

2.3.3.5 Supersingular Elliptic Curve Isogeny Cryptography

Based on the classical ECC concept, which works on defining points evaluated by computing addition and scalar multiplication operations. These points are defined on elliptic curves. Additionally, isogenies define operations between different elliptic curves[138]. Rostovtsev and Stolbunov[7] 2006 introduced public-key cryptosystems based on isogenies. However, more computation time required for encryption and decryption is the major drawback of this scheme. Later in 2010, Jao and Soukharev[129]identified a sub-exponential Quantum Computing attack on this system. Moreover, Isogeny-based schemes may serve as digital signatures or key exchanges[137], such as Supersingular Isogeny Diffie-Hellman (SIDH) and Supersingular Isogeny Key Encapsulation(SIKE) protocols[138].These protocols are basic building blocks featuring different functionalities and levels of security. SIDH and SIKE protocols are to construct efficient and flexible authenticated key exchange schemes. Supersingular elliptic curve isogeny cryptography can facilitate secure key exchange among IoT devices, allowing them to create mutual cryptographic keys to ensure encrypted communication.

2.3.4 Comparison of Quantum Schemes with Classical Schemes

In comparison with classical schemes, the resource requirements of Quantum schemes differ. Table 2.7 represents the juxtaposition of the secret key and message sizes, proposed algorithms, their impact on Quantum Computer and the time taken to execute in a classical computer of selected Post-Quantum schemes.

2.4 Preliminaries

This section also covers the foundational elements necessary for designing and analyzing the schemes presented in subsequent chapters.

2.4.1 BAN Logic

In 1989, Burrows, Abadi, and Needham introduced BAN Logic, a model based on knowledge and belief. This model is intended to describe and validate authentication protocols, specifically aiming to evaluate their security in computer networks or distributed systems. Following authentication, BAN Logic strives to establish the confidence of three entities (individuals, computers, or services) that they communicate with each other rather than potential intruders.

To analyze a protocol using BAN Logic, the protocol is transformed into BAN logic formulas through an ”idealization step.” This involves making reasonable assumptions based on the specific situation and applying logical rules to infer whether the protocol can achieve its intended security goals. The simplicity and practicality of BAN Logic have led to its widespread adoption for protocol analysis.

BAN logic employs the following elements:

1. P believes X: When a party is convinced or authorized to infer the truth of a statement, we describe this as the party holding a belief. Certain beliefs are established

Table 2.7: Comparison of Post-Quantum cryptography schemes with classical cryptography

Proposed Algorithms	**Purpose**	**Public Key - Size(Bytes)**	**Data– Size**	**Time in a classical computer**	**Impact on Quantum Computer**	**Time in Quantum computer**	**Ref.**
Public-Key Signatures							
Hash-based							
XMSS (stateful)	Reduces the signature size of MSS	64	2,500 – 2,820	————	Secure, Not broken by Shor in polynomial time.	The run time <t,x E {0,1}ˆn was selected on a random basis with a uniform distribution.	[139]
SPHINCS (state free)	provide security even against attackers.	1,056	41,000	————-	Against Quantum attacks, expendable 2ˆ128 security is provided.	Signature time depends upon the number of Layers.	[140]
Multivariate based							
HFEv-*	Ability to produce the shortest signature.	500,000 – 1,000,000	25-32	—-	Most promising and Secure but has a large signature as compared to classical schemes.	polynomial Time	[140]
Lattice-based							
BLISS	Based on preimage sample table functions.	—	——	———	Quantum Resistant for constrained IoT Devices.	Ring-LWE provides security higher than 156 bit: 68 ms and 18.8ms for encryption. and decryption	[73]
Public-Key Encryption							
Code based:							
McEliece	Provide codeword based Encryption	958,482 – 1,046,739	187-194	———-	Withstood all proposed attacks, no Quantum attack.	———	[73]
Lattice-based							
NTRUEncrypt with binary Goppa	It gives us very good error correcting capabilities.	1,495 - 2,062	1,495 – 2,062	Difficult to break(Time Undetermined)	Provide Security and concerning parameters size classical schemes grow linearly.	Non –Deterministic Polynomial Time.	[73, 55]
KEY-EXCHANGE							
Lattice-based							
NewHope	Resist Quantum attacks as it is based on Mathematical problem RLWE.	—-	1,824 – 2,048	Undetermined	hard to break	Non-Deterministic polynomial Time hardness.	[134]
Supersingular isogenies							
SIDH	Secure and attack resistant: classical and Quantum	——	564	—-	Secure, provide small message size for key exchange.	——	[55], [134]
Quantum Cryptography	Based						
Quantum Walk	Secured Key exchange	——	——	———	Quantum Resistant	2ˆ305 Keyspace required.	[73]
Classical schemes:							
Symmetric key encryption							
AES-256	Faster and secure Encryption	——	——	Time complexity: - Brute-force attack O(2n). -AES-128bit encryption O(2ˆ128).	Doubling the Key – Size	Time complexity: -AES-128 bit encryption: O(2ˆ64), - Easy to crack by Quantum computer. -Cracked using Brute Force attack O(2ˆn/2).	[73]
Salsa20	symmetric stream ciphers for authenticated encryption construction	——	——	——-	Insecure, the Grover algorithm can break security Salsa 20.	—-	[141]
Asymmetric-Key Encryption							
RSA	Operates on authentication function and Public key cryptosystems.	For RSA-2048: 256 RSA-4096:512	256 and 512	Sub-Exponential Time analysis: C*10ˆ8 for 512 bits and C*10ˆ17 for 1024 bits. Here, C constant.	Completely insecure, solved by Shor's[92]algorithm.	0.5*10ˆ9 and calculated to be 4nˆ3	[73] ,[134]
ECC	Operate on Elliptic Curve equations	For 256 bit -32 512 bit -64	32 and 64	Sub-Exponential-Time analysis: C*10ˆ8 for specific 512 bits and c*10ˆ17 for specific 1024 bits.	Insecure,Shor's algorithm can break ECC.	360nˆ3;n: Number of bits	[73]

as assumptions, while others are logically derived within the framework using predefined postulates.

2. P sees X: Principal P receives a message with X, potentially decrypts it, and can include X in messages to others. X may be a statement or simple data like a nonce.

"Seeing" doesn't automatically mean believing in BAN logic. Messages in a valid protocol should lead to new beliefs for principals to authenticate properly.

3. P said X: At a certain point, Principal P transmitted a message containing statement X. The timing of the message, whether sent in the past or during the ongoing protocol run, is uncertain. However, it is confirmed that P held the belief in X at the time of sending the message.

4. P controls X: P has control over X, and P is a trusted authority on the matter. This is used when a principal delegates authority, such as trusting specific servers to generate encryption keys properly.

5. fresh(X):The formula X is newly generated, meaning it has not been transmitted in any message prior to the ongoing protocol execution. This typically applies to nonces, which are specifically designed to be fresh. Nonces often incorporate a timestamp or a unique number for this purpose.

6. $P \leftrightarrow Q$: P and Q can employ the shared key K for communication. The key K is secure, ensuring that no principal, apart from P or Q, or a principal trusted by P or Q, will ever uncover it. $\{X_K\}$ encrypted with the key K.

Protocol analysis BAN logic can solve four problems in the formal analysis of the protocol:

1. Is this protocol effective?
2. What precisely does this protocol accomplish?
3. Does this protocol require additional assumptions compared to another protocol?
4. Does this protocol perform any superfluous actions?

The main rules for deriving legal annotations are the following:

1. If X holds before the message P → Q: Y, then both X and Q sees Y hold afterwards.
2. If Y can be derived from X by the logical postulates, then Y holds whenever X holds.
3. Step by step, we can follow the evolution from the initial beliefs to the final ones, from the original assumptions to the conclusions.

2.4.2 AVISPA

AVISPA, short for Automated Validation of Internet Security Protocols and Applications, is an automated tool created to validate security-sensitive protocols and applications on the Internet effortlessly. The tool utilizes a flexible formal language to specify protocols and their security properties. It also integrates multiple back-ends with advanced automatic analysis techniques. The AVISPA Tool is structured as represented in Figure2.7.AVISPA offers the HLPSL language to define security protocols and articulate their desired attributes. It also provides a suite of tools for their formal validation. The AVISPA Tool comprises four back-ends: OFMC, CL-AtSe, SATMC, and TA4SP.The HLPSL specification is composed of the following:

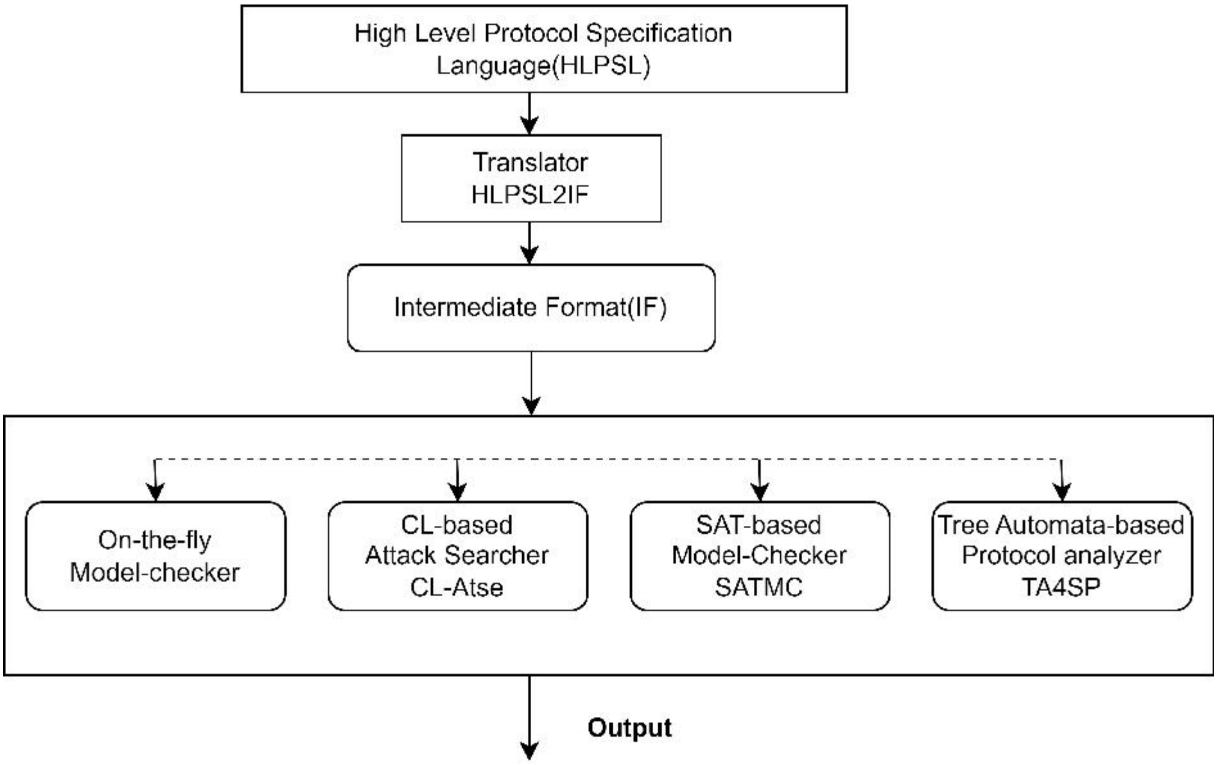

High Level Protocol Specification Language(HLPSL)
Translator HLPSL2IF
Intermediate Format(IF)
On-the-fly Model-checker
CL-based Attack Searcher CL-Atse
SAT-based Model-Checker SATMC
Tree Automata-based Protocol analyzer TA4SP
Output

Figure 2.7: AVISPA Tool Architecture

(a) **Definition of a role:** HLPSL operates as a role-based language, where the actions of each participant type are specified within a module, referred to as a basic role. Translating a protocol into HLPSL is most straightforward when initially expressed in Alice-Bob (A-B) notation. Roles function as separate processes, possessing a designated name, accepting information through parameters, and featuring local declarations. Basic roles are enacted by an agent, whose name is received as a parameter. The activities of a basic role are conveyed through transitions, illustrating alterations in their state based on events or facts.

For example, below, we represent X-Y notation with the well-known Wide Mouth Frog protocol:

$$X- > Z : kxy\_kaz$$

$$Z- > Y : kxy\_kaz$$

In this protocol, A aims to establish a secure session with B by exchanging a novel shared session key through the assistance of a trusted server S, with whom both A and B possess a shared key.

(b) **Transitions**: In HLPSL specifications, the transition section outlines events like message reception and reply sending. Each transition includes a trigger (precondition) and an associated action. For instance, in the server role of our example, a transition is defined.
$State = 0 \wedge RCV(PKxy'\_Pkxz) = | > State' = 2 \wedge SND(PKxy'\_Pkyz) = | >$

In this context, the state is equal to zero, which reflects that the message must be received. It contains some encrypted values. Next, the transaction in the sequence

Shares the received values on the channel with its encryption key.

(c) **Instantiating Sessions**: Creating a session may seem straightforward, but it's often more complex than it appears. Typically, there's a top-level role, often named "environment." In this step, multiple sessions are crated according to the composed roles.

2.4.3 Random Oracle Model (ROM)

The ROM approach is used to prove the security and practicality of a cryptographic scheme, as opposed to the standard model. The concept involves demonstrating the scheme's security by identifying whether it is legitimate or malicious and has access to a public random function. Fiat and Shamir introduces the concept of the ROM approach in 1986

The random oracle operates as a publicly available, deterministic, and evenly distributed random function. It uniformly selects a deterministic length in the output domain to reply to any input inquiry, regardless of the input size. The random oracle model incorporates a publicly accessible random oracle into the conventional model, treating a hash function as an idealized random oracle. Within the ROM approach, the adversary can solely acquire the necessary hash value through the random oracle. Practical applications typically substitute the random oracle with a secure hash function.

2.4.4 IBM Quantum Experience (IQE)

Qiskit is a software development kit available as open-source(SDK) and is a collaborative effort between IBM Research and the Qiskit community, as illustrated in Figure 2.8. This toolkit includes an IBM Quantum Composer, enabling the configuration of quantum gates for qubits, and a simulator for testing configurations before execution on the physical quantum machine.

Table 2.8 represents the effective realization of the Quantum gates on the IBM Quantum Experience.

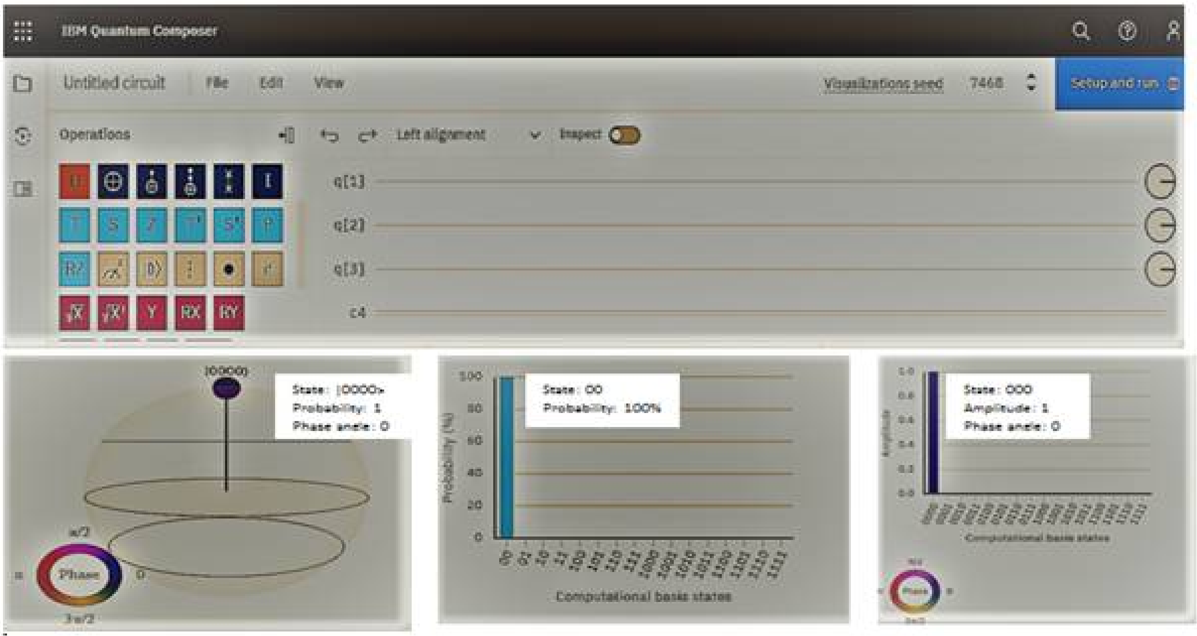
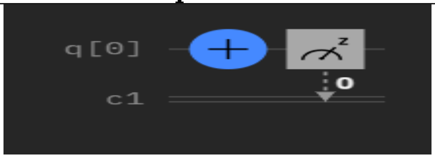
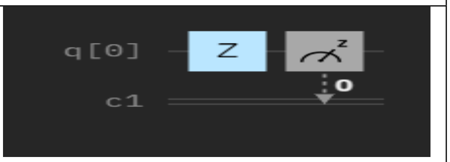
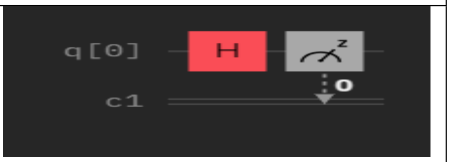
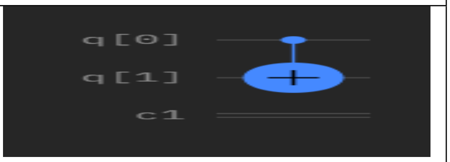
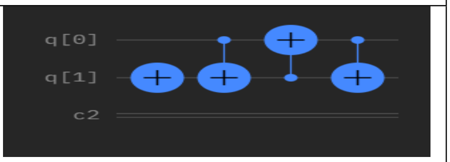


Figure 2.8: IBM Quantum Circuit composer to create Quantum circuits and observe probability outcome, state vector representation and phase representation.

Table 2.8: Single and Multiple Qubits Quantum Gates

Quantum Gate	Matrix Representation	Circuit Representation
NOT(X)-Gate	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	
Phase(Z)-Gate	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	
Hadamard(H)-Gate	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$	
CNOT	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$	
C-SWAP	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	

Chapter 3

MUTUAL AUTHENTICATION AND KEY DISTRIBUTION FOR IoT

In this chapter, we present a Novel Quantum Authentication and Key Agreement (QAKA) protocol that provides unconditional security against any classical and futuristic Quantum threats. The proposed scheme utilizes Quantum Key Distribution(QKD), Greenberger-Horne-Zeilinger states (GHZ) and Quantum Passwords (QP) for securely transferring information in an IoT-enabled communication network.

3.1 Introduction

In this section, we introduce our novel Quantum Authentication and Key Agreement (QAKA) Protocol, considering the constraints of classical cryptographic methods and drawing inspiration from the potential benefits of Quantum Cryptography[142]. In our protocol, the user and Quantum Sensor Node(QSN) authenticate via a secure GWN before communication occurs. Each user must register onto GWN before receiving data from legitimate QSN. The user login and authentication process occurs by QGC, issued to legitimate users. The QSN must register onto GWN before sending perceived data to legitimate users. Quantum Authenticated Channel (QAC) prevents eavesdropping in our protocol.Our scheme can withstand classical attacks such as replay, eavesdropping, Man-in-Middle (MITM), traffic analysis and futuristic Quantum attacks. Hence, QAKA guarantees secure key management, mutual authentication, confidentiality, integrity and reliability when users access IoT-enabled networks.

3.1.1 System Model

The proposed system model consists of three entities User, Gateway node and Sensor node.In our scheme, the Gateway is a trusted entity onto which each user and sensor node registers them before establishing any secure communication.In this system model, the users and sensor Node register themselves onto the Gateway Node by generating the secure Quantum Key. After that, the Gateway node issues the QGC to legitimate users as represented in Figure 3.1. The Unique Quantum Password (QP) is provided to authorized users whenever the user logs into the system by securely generating Quantum Key with Gateway Node.

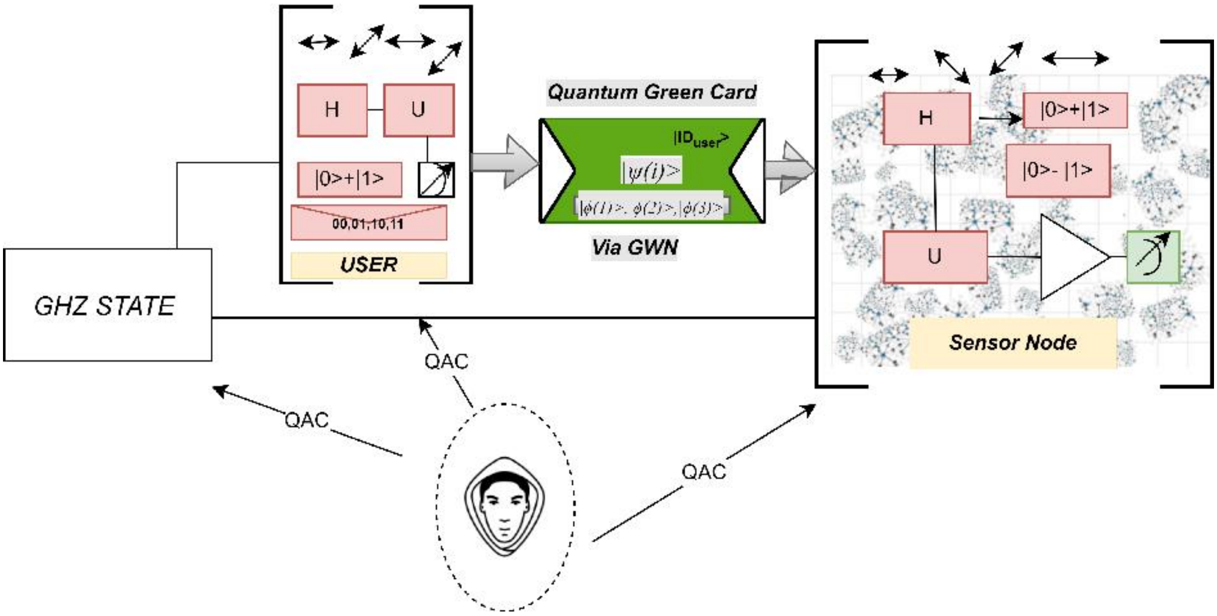


Figure 3.1: QAKA Architecture

3.1.2 Threat Model

In this model, we consider that the IoT communication framework is inherently vulnerable to attacks due to open Internet connectivity. The data collected from sensor nodes and devices in the IoT framework provide sensitive information and without secure mutually authenticated protocol, such schemes are supposed to be compromised.The sensor nodes provide critical information from the unguarded locations where the adversary can perform false data injection attacks. The intruder can also obtain the user's secret information communicated over the insecure channel and can perform intercept, resend, insert and delete messages. We have considered various threats to the IoT communication framework. In the proposed scheme, it is imperative to fulfil fundamental security prerequisites, including user authentication and the establishment of secure keys, in order to guarantee secure communication among the User, Gateway, and Sensor Node.

3.2 Proposed Quantum Authentication and Key Agreement(QAKA) Protocol

In this section, we present the proposed QAKA protocol. The QAKA protocol comprises four algorithms: GEN, registration, login and authentication. The five phases of our proposed protocol are as π =(Pre-Deployment, GEN, REG, login, Auth.).These phases are described as follows:

3.2.1 Pre-Deployment Phase

Before deploying the QSN, the network administrator assigns a secure and unique ID_{SN} during the pre-deployment phase. The QSNs possess constrained resources and are pre-installed in an unattended environment, while the gateway node is well-equipped[102]. Therefore, GWN stores $|ID_{QSN}\rangle$ of QSN in its database. Each legal user is provided with a unique ID as $|ID_{USER}\rangle$. In addition to that, an authenticated user has to share some unique information about their device, like a mobile phone or PDA, with a verifier for authentication purposes in future network communication. In the IoT-enabled communication environment, all this information must be saved in GWN.

3.2.2 GEN Algorithm Phase

Our protocol is based on GHZ states that can entangle more than two qubits. We introduced four-particle GHZ states with three communicating parties to describe the IoT communication process User, QSN and Gateway. In our protocol, GWN is an authenticated entity and created GHZ states with all other entities involved in communication. In Eq3.1, the mathematics of GHZ state preparation is presented. The Hadamard gate, when applied on the initial Qubit state $|0\rangle$, generates the superposition of states. Such a state, when entangled with other qubits by applying unitary Quantum gates, generates the final maximally entangled states.

On IBM Quantum Composer (IQC), the maximally entangled states can be obtained by applying Quantum H-Gate and CNOT Gate, as depicted in Figure 3.2.
S1= $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \bigotimes |000\rangle = \frac{1}{\sqrt{2}}(|0000\rangle + |1000\rangle)$
S2 $= U_{CNOT}^{ctrl=q1}|S1\rangle = \frac{1}{\sqrt{2}}(|0000\rangle + |1100\rangle)$
S3 $= U_{CNOT}^{ctrl=q1}|S2\rangle = \frac{1}{\sqrt{2}}(|0000\rangle + |1110\rangle)$
S4 $= U_{CNOT}^{ctrl=q1}|S3\rangle = \frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle)$

$$|\phi_{GHZ}^{(i)}\rangle = \frac{1}{\sqrt{2}}(|0^{(i)}\rangle_{U1}|0^{(i)}\rangle_{U2}|0^{(i)}\rangle_{GW}|0^{(i)}\rangle_{SN} + |1^{(i)}\rangle_{U1}|1^{(i)}\rangle_{U2}|1^{(i)}\rangle_{GW}|1^{(i)}\rangle_{SN}) \tag{3.1}$$

Where, $1 \leq i \leq n$, denotes the specific and individual identifier for each communicating entity $i\epsilon\{0,1\}^n$. Here,$\{|\phi_{GHZ}^{(i)}\rangle\}_{i=1:m} = |\phi_{GHZ}^{(1)}\rangle$,$|\phi_{GHZ}^{(2)}\rangle$....$|\phi_{GHZ}^{(m)}\rangle$ symbolizes maximally entangled states. Every time a user logs into the system, a distinct GHZ state is created. Using the GHZ state, GWN prepares entangled qubits with the user and QSN.

3.2.3 User Registration Phase

Prior to communication, users undergo identity registration with the GWN in this phase.To register, users need to adhere to the subsequent steps:
Step 1: User input credentials:$|ID_{USER}\rangle$ into GWN.
Step 2: GHZ states are generated by GWN upon receiving the user input.
Step 3: Before the registration process, each user receives a distinct Unique ID, using which the User compute $A_i = f(ID_{USER}\|Puk)$. A user sends this information to the Gateway Node for verification.
Step 4: Initially, GWN has the following credentials as $|ID_{USER}\rangle$ .Gateway Node checks the information received from the user by evaluating the Quantum One-Way function (QOWF) as in Eq3.2:

$$A_i^{'} = f(ID_{USER}\|Puk) \tag{3.2}$$

Where ID_{USER} represents the user identity, Puk is the public key of the user, and $\|$ concatenates two-bit strings. If the information in Eq3.2 matches, then upon receiving the public key (puk) from the user, GWN compute:

$$B_i = f(ID_{USER}\|Prk)$$

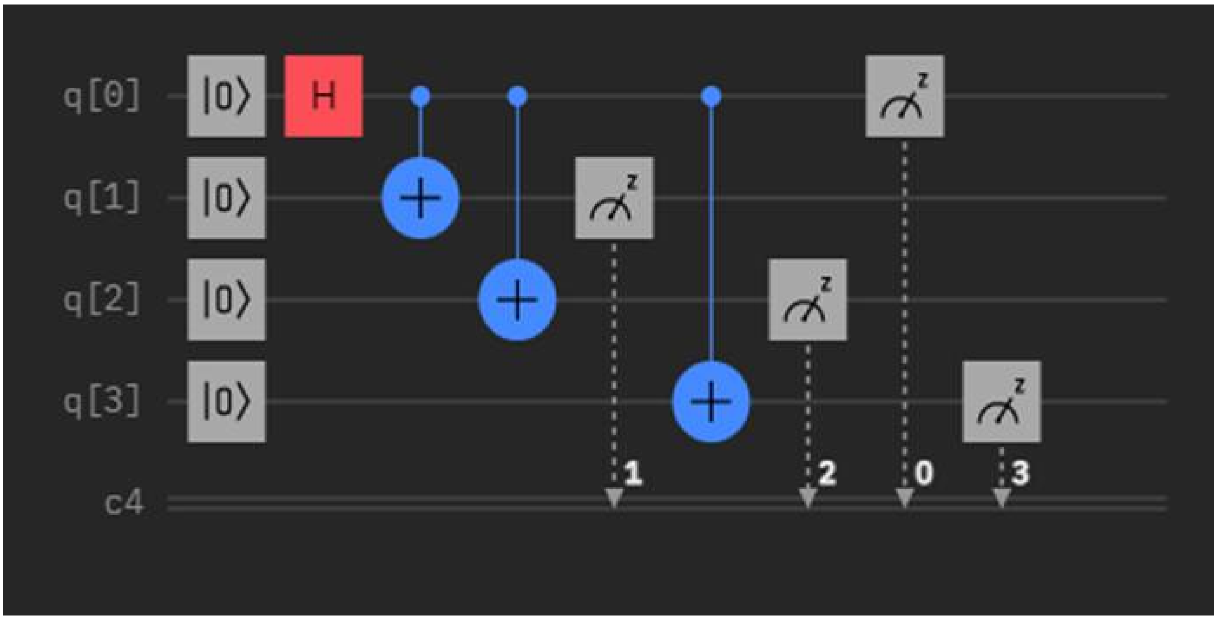


Figure 3.2: GHZ states by using CNOT and Hadamard Gate

and send B_i to User.
Where,ID_{USER} represents the user identity, and Prk is the private key of the user.
Step 5: Both GWN and user prepare a shared key (sk), $sk\epsilon\{0,1\}^L$. The shared key can be effectively realized using QKD protocol, BB84[143].
Step 6: The user prepares the state, $|\psi^{(i)}_{UIN}\rangle = f(ID_{USER}\|sk)$,it contains the user information(UIN) and store in its Quantum Memory.
Step 7: The user information, along with the public key, is secured as in Eq.3.3:

$$|\psi_{USER}\rangle = f(ID_{USER}\|Puk) \tag{3.3}$$

Step 8: The transformed state can be written in Eq3.4.

$$|\phi^{(i)}\rangle = |\psi_{USER}\rangle \otimes |\phi\rangle$$

$$= \frac{1}{\sqrt{2}}\{|\Phi^+\rangle_{U1}(\beta|0_{U2}0_{GW}0_{SN}\rangle+\alpha|1_{U2}1_{GW}1_{SN}\rangle)+|\Phi^-\rangle_{U1}(\beta|0_{U2}0_{GW}0_{SN}\rangle-\alpha|1_{U2}1_{GW}1_{SN}\rangle)+$$
$$|\Psi^+\rangle_{U1}(\alpha|0_{U2}0_{GW}0_{SN}\rangle + \beta|1_{U2}1_{GW}1_{SN}\rangle)+$$
$$|\Psi^-\rangle_{U1}(\alpha|0_{U2}0_{GW}0_{SN}\rangle - \beta|1_{U2}1_{GW}1_{SN}\rangle)\} \tag{3.4}$$

Where $|\psi_{USER}\rangle$ represents the important user credentials as in Eq.3.3, $|\phi\rangle_{GHZ}$ represents the $|\phi^{(i)}\rangle_{U1}$ as in Eq.3.1,$\otimes$ represents the tensor product between the qubits and $|\Phi^{\pm}\rangle$ $=\frac{|00\rangle\pm|11\rangle}{\sqrt{2}}$ $|\Psi^{\pm}\rangle$ $=\frac{|10\rangle\pm|01\rangle}{\sqrt{2}}$ signify one of the four quantum bell states, measured by the user.
Step 9: Following the encoding process, the user proceeds to measure their portion of the second qubit $|\phi^{(i)}_{U2}\rangle$ as represented in Eq.3.1. The measurement results are as $\{00, 01, 10, 11\}_{c1,c0}$ the user applies a Pauli matrix (error correction)[144] on the entangled part of the qubits, which is in his possession $|\phi^{(i)}\rangle_{U2}$ as:

$$|\Psi^+\rangle \rightarrow I; \quad |\Psi^-\rangle \rightarrow Z; \quad |\Phi^+\rangle \rightarrow X; \quad |\Phi^-\rangle \rightarrow Y$$

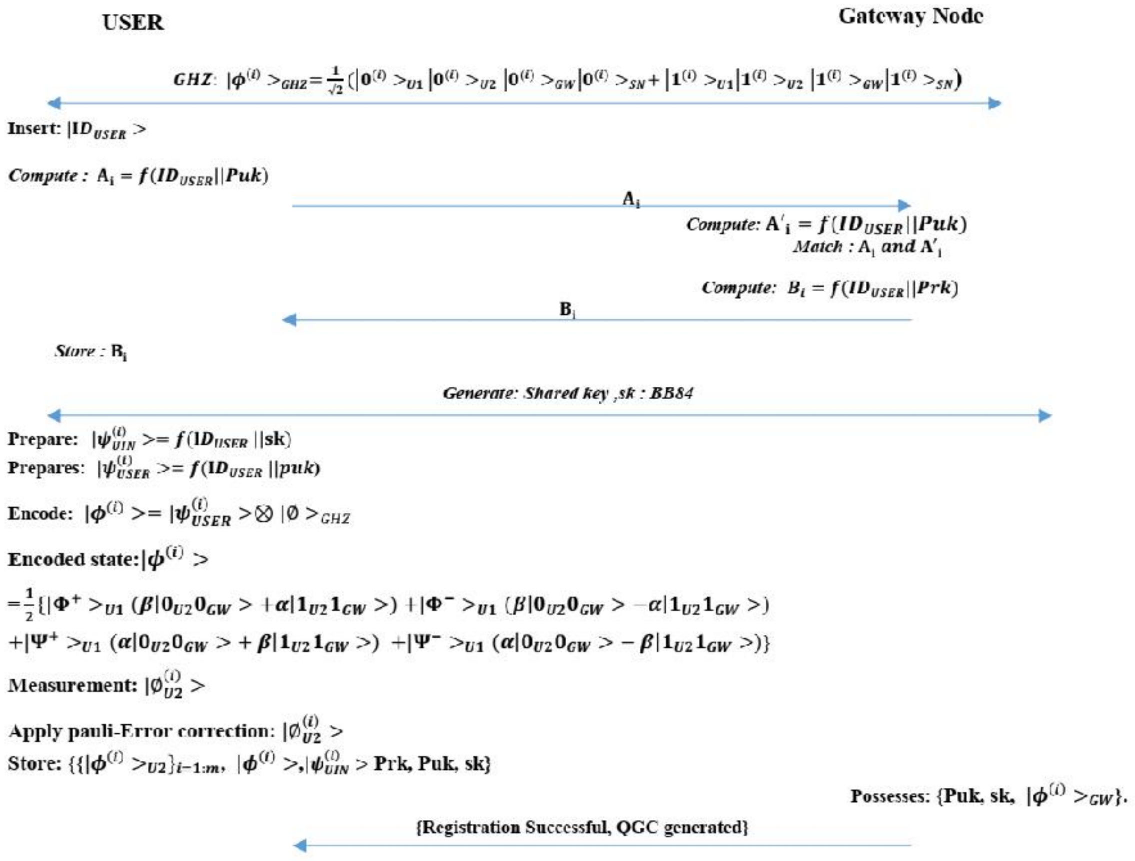

USER
Gateway Node
GHZ: $|\phi^{(i)}>_{GHZ}=\frac{1}{\sqrt{2}}(|0^{(i)}>_{U1}|0^{(i)}>_{U2}|0^{(i)}>_{GW}|0^{(i)}>_{SN}+|1^{(i)}>_{U1}|1^{(i)}>_{U2}|1^{(i)}>_{GW}|1^{(i)}>_{SN})$
Insert: $|ID_{USER}>$
Compute : $A_i = f(ID_{USER}||Puk)$
A_i
Compute: $A'_i = f(ID_{USER}||Puk)$
Match : A_i and A'_i
Compute: $B_i = f(ID_{USER}||Prk)$
B_i
Store : B_i
Generate: Shared key ,sk : BB84
Prepare: $|\psi^{(i)}_{UIN}>= f(ID_{USER}||sk)$
Prepares: $|\psi^{(i)}_{USER}>= f(ID_{USER}||puk)$
Encode: $|\phi^{(i)}>= |\psi^{(i)}_{USER}>\otimes|\emptyset>_{GHZ}$
Encoded state:$|\phi^{(i)}>$
$=\frac{1}{2}\{|\Phi^{+}>_{U1}(\beta|0_{U2}0_{GW}>+\alpha|1_{U2}1_{GW}>)+|\Phi^{-}>_{U1}(\beta|0_{U2}0_{GW}>-\alpha|1_{U2}1_{GW}>)$
$+|\Psi^{+}>_{U1}(\alpha|0_{U2}0_{GW}>+\beta|1_{U2}1_{GW}>)+|\Psi^{-}>_{U1}(\alpha|0_{U2}0_{GW}>-\beta|1_{U2}1_{GW}>)\}$
Measurement: $|\emptyset^{(i)}_{U2}>$
Apply pauli-Error correction: $|\emptyset^{(i)}_{U2}>$
Store: $\{\{|\phi^{(i)}>_{U2}\}_{i-1:m}, |\phi^{(i)}>, |\psi^{(i)}_{UIN}>$ Prk, Puk, sk$\}$
Possesses: {Puk, sk, $|\phi^{(i)}>_{GW}$}.
{Registration Successful, QGC generated}

Figure 3.3: QAKA protocol user registration

.

The user holds the following information:
$\{\{|\phi^{(i)}\rangle_{U1}$,$|\phi^{(i)}\rangle_{U2}\}_{i=1:m}$,Puk,Prk,sk,$|\psi^{(i)}_{UIN}\rangle\}$ and GWN holds the following information as: {Puk,sk,$|\phi^{(i)}_{GW}\rangle$}.
Where, $|\phi^{(i)}\rangle_{GW}$,$|\phi^{(i)}\rangle_{U1}$,$|\phi^{(i)}\rangle_{U2}$ are GWN and legal users GHZ particles as represented in Eq. (7), public key (Puk), private key (Prk), shared key (sk), $|\psi^{(i)}_{UIN}\rangle$ is user-generated information as represented in Step 6.
Following the provided details, the user undergoes registration with the GWN. Following a successful registration, an individualized QGC is created for each authorized user, encompassing their pertinent information, including:
$\{\{|\phi^{(i)}\rangle_{U1}$, $|\phi^{(i)}\rangle_{U2}\}_{i=1:m}$, Puk,Prk,sk,$|\psi^{(i)}_{UIN}\rangle\}$ for secure login.The QGC is furnished with Quantum storage, which can be employed for subsequent secure communications. The user registration phase has been summarized in Figure 3.3

3.2.4 Quantum Sensor Node Registration Phase

In this phase, the QSN register them onto GWN using the quantum channel before providing information to the user. Figure 3.4 represents the steps required for QSN registration onto GWN, and the description is explained as follows:
Step 1: QSN has the unique identity as $|ID_{QSN}\rangle$.The Quantum Sensor Network (QSN) performs measurements in the H-Basis and transmits the measurement outcomes to GWN.

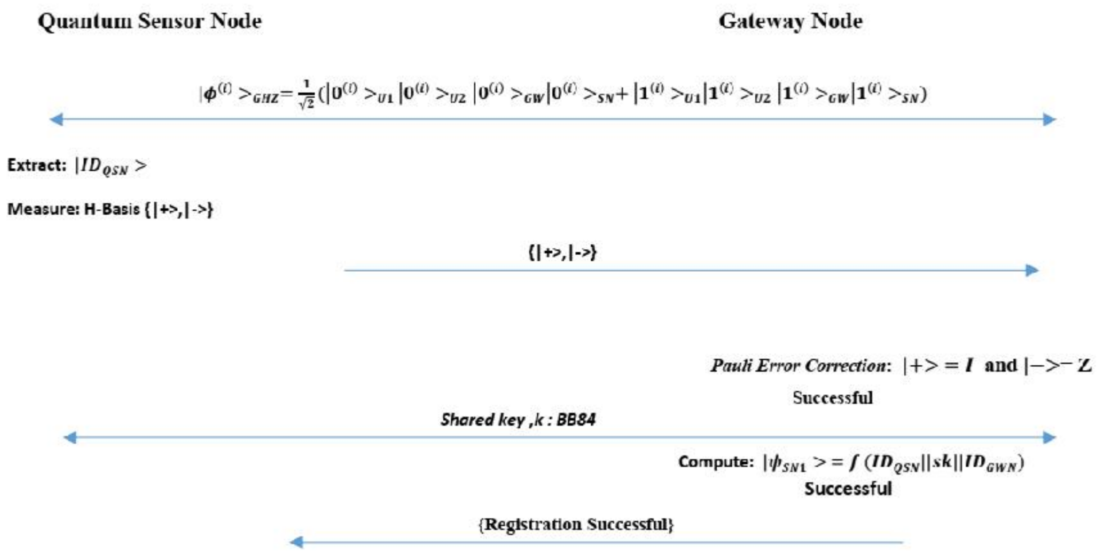

Quantum Sensor Node
Gateway Node
$|\phi^{(i)}>_{GHZ}=\frac{1}{\sqrt{2}}(|0^{(i)}>_{U1}|0^{(i)}>_{U2}|0^{(i)}>_{GW}|0^{(i)}>_{SN}+|1^{(i)}>_{U1}|1^{(i)}>_{U2}|1^{(i)}>_{GW}|1^{(i)}>_{SN})$
Extract: $|ID_{QSN}>$
Measure: H-Basis {|+>,|->}
{|+>,|->}
Pauli Error Correction: $|+> = I$ and $|->- Z$
Successful
Shared key ,k : BB84
Compute: $|\psi_{SN1}> = f\,(ID_{QSN}||sk||ID_{GWN})$
Successful
{Registration Successful}

Figure 3.4: QSN registration in QAKA protocol.

as $|+\rangle$ and $|-\rangle$.

Step 2: Upon receiving information from the Sensor Node, GWN applies Pauli gates as:

$$|+\rangle = I \qquad and \qquad |-\rangle = Z$$

Step 3: With the information provided earlier, the GWN validates the identity of an authorized QSN.

Step 4: If the above step is successful, a shared key, sk, is prepared between QSN and gateway node, using BB84 protocol.

Step 5: Finally, GWN compute the Sensor Node and store it in its database as $|\psi_{SN1}\rangle$= $f(ID_{QSN}\|sk\|ID_{GWN})$, Where, $\{|\psi_{SN1}\rangle\}$ representing the information computed by GWN for successful registration of QSN, it contains Quantum Sensor Node Identity (ID_{QSN}), Gateway Node Identity (ID_{GWN}) and shared key(sk).

Step 6: If the above steps are computed successfully, QSN gets registered to GWN.

3.2.5 User Login Phase

User executes the following steps to securely login in GWN.The steps to be performed for user login are represented in Figure 3.5.

Step 1: The input details as: $|ID_{USER}\rangle$ along with QGC produced by the user.

Step 2: The GWN verifies the shared key (sk) with the user, and a successful match allows the user to retrieve Quantum Password (QP) to securely login into the system.

Step 3: The QP allow the user to retrieve the information from the QSN via GWN.

Step 4: The legitimate user login using the following information securely onto GWN as: $\{|ID_{USER}\rangle$,$|\phi_{QP}\rangle\}$, Where,$|ID_{USER}\rangle$ is user identity and $|\phi_{QP}\rangle$ is Quantum Password.

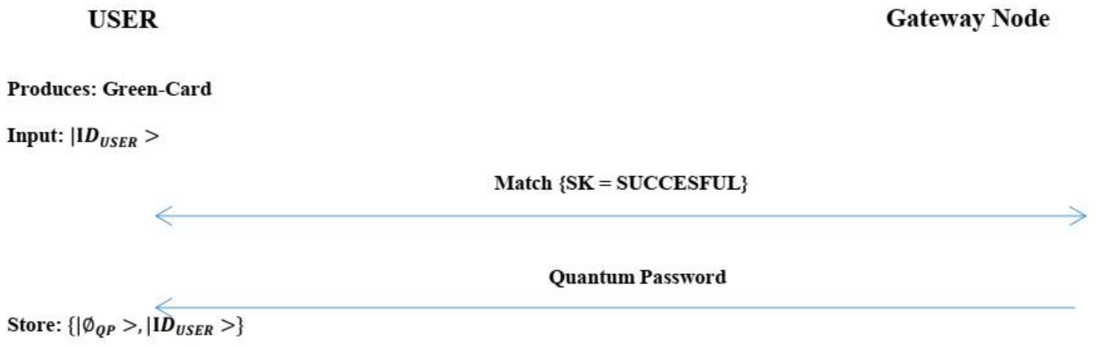


Figure 3.5: User Login process in QAKA protocol.

3.2.6 Authentication Phase

In this process, whenever any user (Prover1) tries to log in to collect information from the QSN, he must prove his identity to the QSN via GWN. The GWN must allow only authenticated QSN (Prover2) to share data with legitimate users. The steps to be performed for verification are illustrated in Figure 3.6.
The verification process is discussed as follows:
Step 1: User produces QGC to GWN and inputs QP. User verification is run using $|\phi^{(i)}_{U2}\rangle$, representing the maximally entangled user particle. The encoded state contains user-important credentials such as $|ID_{USER}\rangle$.
Step 2: The GWN stores the encoded state $|\phi^{(i)}_{U2}\rangle$ in its Quantum memory for retrieval of important user credentials. The GWN verifies the sk generated between the User and GWN. Based on the information encoded in this state, GWN allows legitimate users [Prover 1] to retrieve the data from the QSN securely.
Step 3: GWN authenticates QSN by verifying the shared key, sk [Prover 1].
Step 4: If the step 3 is successful, then GWN send the following user information to QSN as $\{|\phi^{(i)}\rangle_{U2}\}$.
Step 5: GWN measures its state $|\phi^{(i)}_{GW}\rangle$ in H-Basis $\{|+\rangle, |-\rangle\}$ and sends the measurement results to QSN for verifying user identity $\{|\phi^{(i)}\rangle_{U2}\}$.
Step 6: QSN applies the appropriate correction Gate on an unknown state $|\phi^{(i)}\rangle_{U2}$ based on the measurement outcome as received from GWN as: $\{|+\rangle = I, |-\rangle = Z\}$
Step 7: The QSN also computes the state of the system as $|\psi_{SN2}\rangle = f(ID_{GWN}\|ID_{QSN}\|ID_{USER})$.
Step 8: The user based on the retrieved information matches $|ID_{USER}\rangle$ and compute User state $|\psi_{US}\rangle = f(ID_{USER}\|ID_{QSN})$
Step 9: GWN subsequently employs the SWAP Test on $\{|\psi^{(i)}_{UIN}\rangle|\psi'^{(i)}_{UIN}\rangle\}$ for verification of each user login into the system. It also verifies $\{|\psi_{SN1}\rangle|\psi'_{SN1}\rangle\}$ to authenticate the valid QSN.
The figure depicts the SWAP gate 3.7. It indicates whether two states are identical if $|q_0\rangle = |0\rangle$. However, if $|q_0\rangle = |0\rangle$ or $|1\rangle$ with same likelihood.The Orthogonality is proved. The equality of both states hinges on the outcome of measurement, as described in Eq.3.5.

$$P(1) = \frac{1}{2}(1 - | < \phi|\psi > |^2) \quad and \quad P(0) = \frac{1}{2}(1 + | < \phi|\psi > |^2) \tag{3.5}$$

In this context, $| < \phi|\psi > |^2$ signifies the square of the probability amplitudes for two distinct states, where P (1) represents the likelihood of measuring 1 on $|q_0\rangle$ and $P(0)$ is

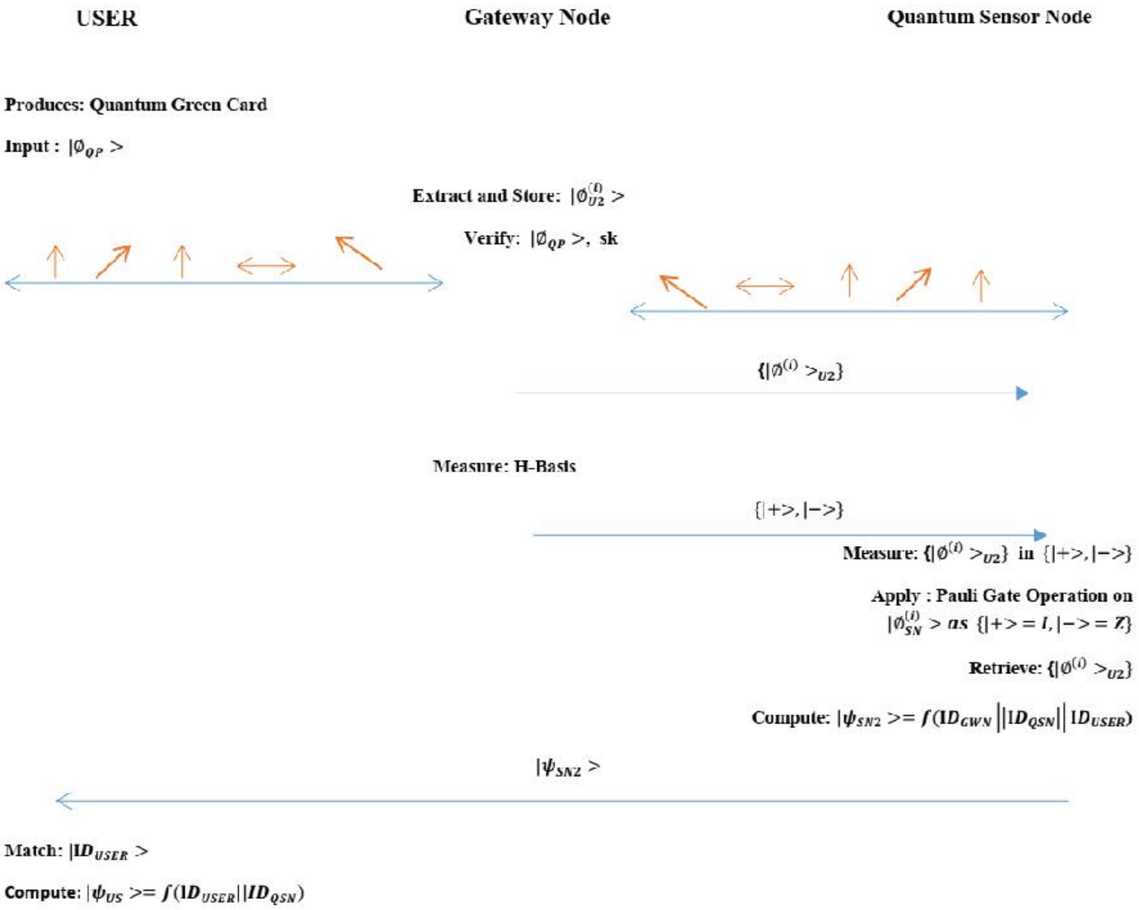

USER
Gateway Node
Quantum Sensor Node
Produces: Quantum Green Card
Input : $|\emptyset_{QP}>$
Extract and Store: $|\emptyset^{(i)}_{U2}>$
Verify: $|\emptyset_{QP}>$, sk
$\{|\emptyset^{(i)}>_{U2}\}$
Measure: H-Basis
$\{|+>, |->\}$
Measure: $\{|\emptyset^{(i)}>_{U2}\}$ in $\{|+>, |->\}$
Apply : Pauli Gate Operation on $|\emptyset^{(i)}_{SN}>$ as $\{|+> = I, |-> = Z\}$
Retrieve: $\{|\emptyset^{(i)}>_{U2}\}$
Compute: $|\psi_{SN2}>= f(ID_{GWN}||ID_{QSN}||ID_{USER})$
$|\psi_{SN2}>$
Match: $|ID_{USER}>$
Compute: $|\psi_{US}>= f(ID_{USER}||ID_{QSN})$

Figure 3.6: Authentication process in QAKA protocol.

the likelihood of measuring $|0\rangle$ on the first qubit. Two states are identical if: $P(1)$=0 and $P(0)$=1. However, if $P(0) < 1$ then states are not identical as depicted in Figure3.7

However, in cases where the states do not align, the ancilla qubits are in a superposition, existing in both $|0\rangle$ and $|1\rangle$ states. The GWN evaluates the likelihoods linked to each possible result. The GWN analyze the likelihood associated with each outcome as $\{|\psi^{(i)}_{UIN}\rangle|\psi'^{(i)}_{UIN}\rangle\} \geqslant \eta_1$ and $\{|\psi_{SN1}\rangle|\psi'_{SN1}\rangle\} \geqslant \eta_2$,where $\eta_1$and η_2 constants decided by GWN.
Here, η_1 and η_2 are constant and fixed by GWN. The process must be repeated for each entity that desires to obtain information from the QSN. Else, GWN will terminate the process. Session Key (SK) is established after proper mutual authentication between communicating entities.

The Flow diagram of the Authentication phase is depicted in Figure3.8

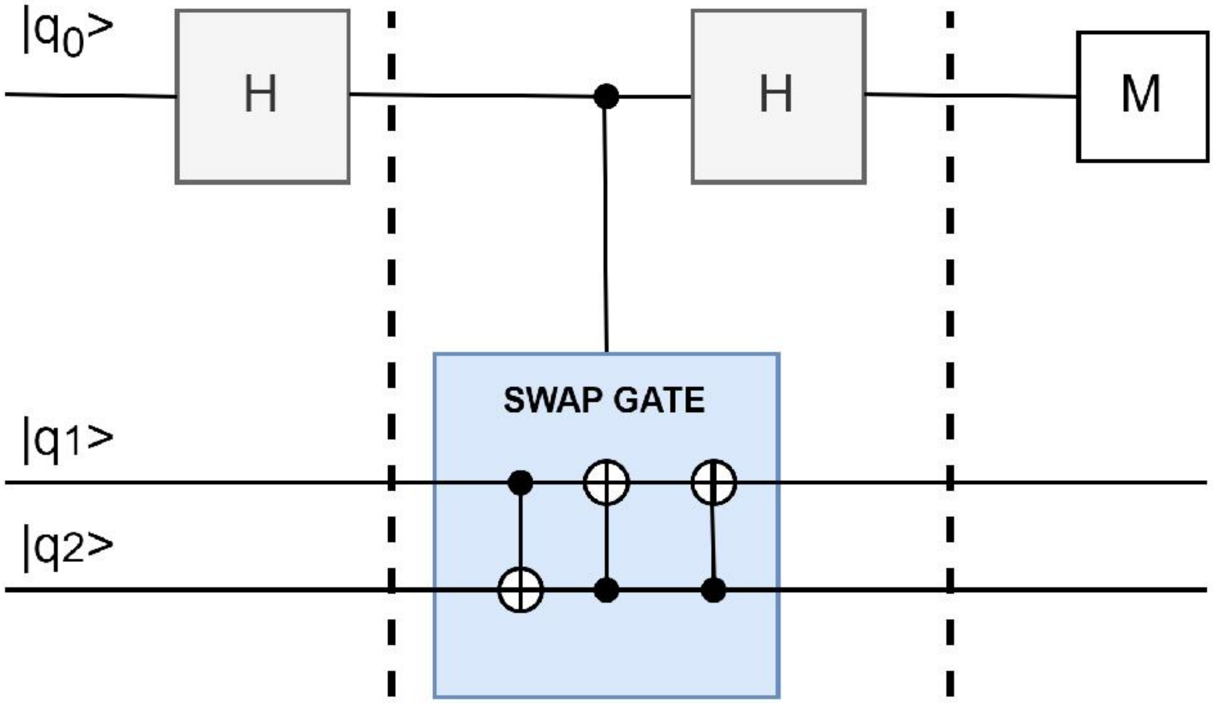


Figure 3.7: Quantum SWAP Circuit.

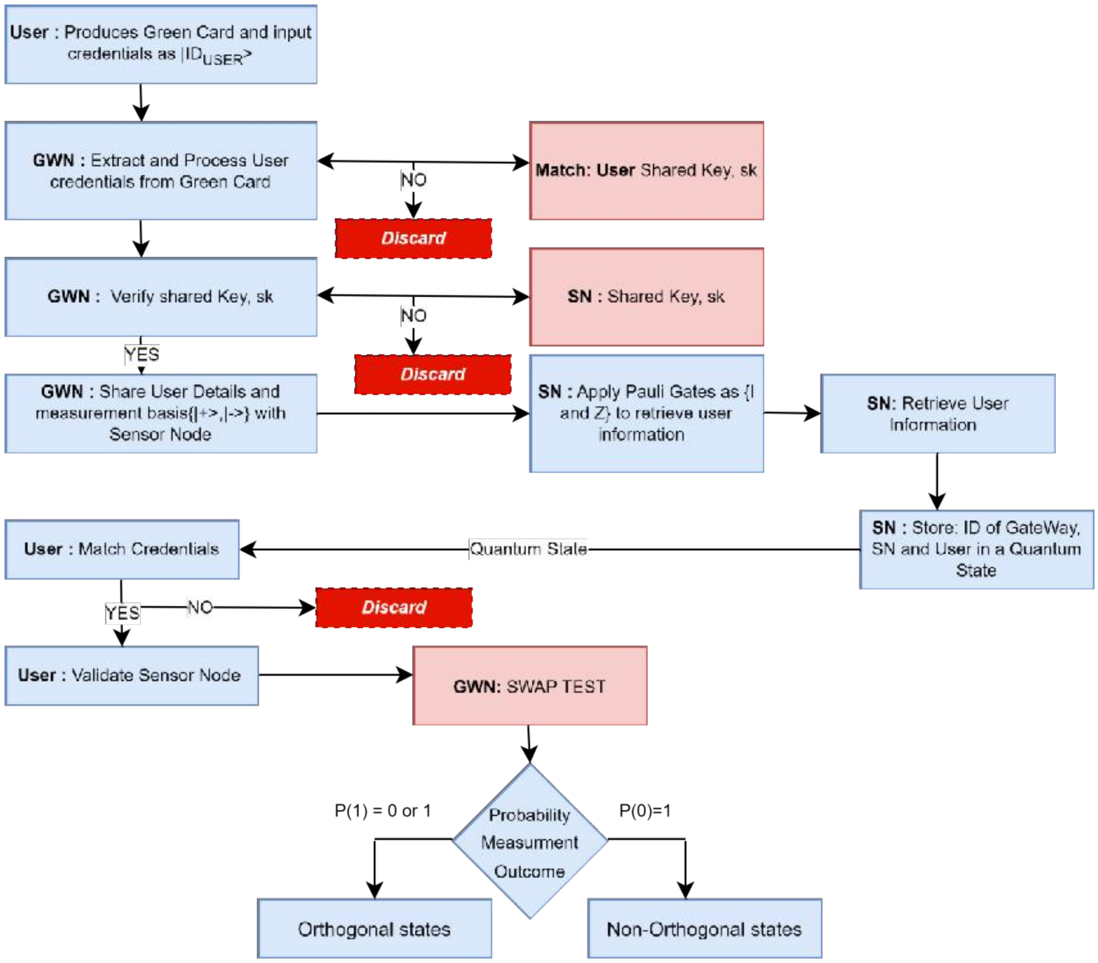

User : Produces Green Card and input credentials as |IDUSER>
GWN : Extract and Process User credentials from Green Card
Match: User Shared Key, sk
NO
Discard
GWN : Verify shared Key, sk
SN : Shared Key, sk
NO
Discard
YES
GWN : Share User Details and measurement basis{|+>,|->} with Sensor Node
SN : Apply Pauli Gates as {I and Z} to retrieve user information
SN: Retrieve User Information
SN : Store: ID of GateWay, SN and User in a Quantum State
Quantum State
User : Match Credentials
YES
NO
Discard
User : Validate Sensor Node
GWN: SWAP TEST
P(1) = 0 or 1
Probability Measurment Outcome
P(0)=1
Orthogonal states
Non-Orthogonal states

Figure 3.8: Flow graph of the QAKA scheme.

3.3 Security Analysis

BAN logic serves as a framework for security assessments of authentication protocols, and it has received validation and application in prior schemes, as evidenced by references [94, 145]. In this section, we analyze the security of the proposed QAKA protocol using a formal analysis of BAN and ROM. We also present the informal analysis of the proposed scheme.

3.3.1 QAKA Formal Proof using BAN Logic

In our protocol, the user, GWN, and SN will reach a consensus on both the Quantum secret key and identity. We establish fundamental notations outlined in Table 3.1 to define rules, make assumptions, and offer proofs using BAN logic. In this context, M and V represent statements, while principles are denoted as S and T.

The formulated rules in our work are described as:

- A1: Message –Meaning Rule: $\frac{S|\equiv T\ S\overset{sk}{\longleftrightarrow}T, S\lhd\{M\}_{k_{bs}}}{S|\equiv T|\sim M}$
- A2: Nonce verification rule:$\frac{S|\equiv T\#(M), S|\equiv T|\sim M}{S|\equiv T|\equiv M}$
- A3: Jurisdiction rule:$\frac{S|\equiv T|\Rightarrow M, S|\equiv T|\equiv M}{S|\equiv M}$
- A4: Freshness Rule: $\frac{S|\equiv\#(M)}{S|\equiv\#(M,V)}$
- A5: Shared key rule: $\frac{S|\equiv\#(M), S|\equiv T|\equiv M}{S|\equiv S\overset{sk}{\longleftrightarrow}T}$
- A6: Believe Rule: $\frac{S|\equiv(M,V)}{S|\equiv M}$

The QAKA protocol is deemed secure and legitimate, and in accordance with BAN logic, it must fulfil the following objectives:

- Goal 1: $USER| \equiv (GWN \overset{sk}{\leftrightarrow} USER)$
- Goal 2: $USER| \equiv GWN| \equiv (GWN \overset{sk}{\leftrightarrow} USER)$
- Goal 3: $GWN| \equiv (SN \overset{ID}{\longleftrightarrow} GWN)$
- Goal 4: $SN| \equiv GWN| \equiv (GWN \overset{sk}{\leftrightarrow} SN)$
- Goal 5: $USER| \equiv SN| \equiv (USER \overset{ID}{\longleftrightarrow} SN)$
- Goal 6: $GWN| \equiv (USER \overset{ID}{\longleftrightarrow} GWN)$
- Goal 7: $SN| \equiv USER| \equiv (USER \overset{ID}{\longleftrightarrow} SN)$

The idealised form of QAKA is analyzed considering the messages exchanged using BAN logic as stated below:

- M1: $USER \rightarrow GWN : (USER \overset{sk}{\leftrightarrow} GWN)_{Bs'UG}, (USER \xleftrightarrow{ID_{QGC}} GWN)_{|\phi^{(i)}\rangle_{U2}}$.

Table 3.1: BAN Logic Notations

Symbolism	**Significance**
$S\| \equiv M$	S believes M
S $\lhd$ M	S receives/Sees M
$S\| \sim M$	S sometimes stated M
$S\| \Rightarrow M$	S has complete authority over M
$\#(M)$	M is fresh
$(S \overset{k}{\leftrightarrow} T)$	S and T communicate using shared key K
(M,V)	The formulas are combined and then hashed.
{M} $_k$	M is encrypted with key k
sk	Secret key
k_{as}	Public Key
k_{bs}	Private key
$S_- > T :?$	S sends T? through Quantum Link
$C_1(X), C_2(X), C_3(X)$	Entangled String shared with User, GWN and Sensor Node.
Bs_U, Bs_G, Bs_S	User, Sensor and Gateway Basis
$\updownarrow\nearrow\leftrightarrow\nearrow$	Polarization angles $0^0, 90^0, 45^0, 135^0$

- M2: $GWN \rightarrow SN : (SN \overset{ID}{\longleftrightarrow} GWN)_{|\phi^{(i)}\rangle_{U2}}$,$(SN \overset{sk}{\longleftrightarrow} GWN)_{Bs'SG}$

- M3: $SN \rightarrow USER : (SN \overset{ID}{\longleftrightarrow} USER)_{|\psi_{SN2}\rangle}, (USER \overset{sk}{\longleftrightarrow} GWN)_{Bs'UG}$

We listed some of the assumptions from H11 to H33, which are considered to prove the goals are written as follows:

- H1:$GWN| \equiv (USER \overset{A_i}{\longleftrightarrow} GWN)$: As evaluated in $A_i = h(ID_{USER}||Puk)$, GWN on the belief the User shares the secret.

- H2:$USER| \equiv (GWN \overset{A_i'}{\longleftrightarrow} USER)$: User believes that GWN checks the validity of the message by evaluating $A_i' = h(ID_{USER}||Puk)$.

- H3: $USER| \equiv (GWN \overset{B_i}{\longleftrightarrow} USER)$: User believes that GWN and USER have the same message by extracting information from $B_i = h(ID_{USER} \| Prk)$.

- H4: $USER| \equiv \leftrightarrow \nearrow \updownarrow \nwarrow$: $USER| \Rightarrow (\leftrightarrow \nearrow \updownarrow \nwarrow)$: User believes on the basis and has complete jurisdiction over the basis state.

- H5: $USER| \equiv USER \overset{sk}{\longleftrightarrow} GWN$: The user believes that the secret key(sk) is generated between the user and GWN by exchanging basis state.

- H6: $GWN| \equiv \updownarrow \nearrow \leftrightarrow \nwarrow$ $GWN| \equiv USER \Rightarrow (\leftrightarrow \nearrow \updownarrow \nwarrow)$: GWN believes USER and both agree on the same polarization state.

- H7: $USER| \equiv \#(sk)$:The user believe that the sk is fresh.

- H8: $GWN| \equiv \#(sk)$:GWN believe that the sk is fresh.

- H9:$GWN| \equiv (GWN \overset{sk}{\longleftrightarrow} USER)$: Since both user and GWN agree on a shared basis, they agree on an sk.

- H10: $USER| \equiv GWN| \Rightarrow USER \overset{ID}{\longleftrightarrow} GWN$: By evaluating the User state as $|\psi_{UIN}^{(i)}\rangle = f(ID_{USER} \| sk)$, User can believe that GWN has jurisdiction over the fact that GWN and User share the same identity.

- H11:$USER| \equiv \#(Bs_G)$: Users believe that the basis shared by GWN is fresh.

- H12:$GWN| \equiv \#(Bs_U)$: GWN believes that the basis shared by the User is fresh.

- H13:$USER \overset{sk}{\longleftrightarrow} GWN| \equiv (USER \overset{sk}{\longleftrightarrow} GWN)_{Bs'GU}$: User and GWN communicate using the secret key generated by deleting an unmatched basis.

- H14: $GWN \xleftrightarrow{(ID)_{XYZ}} USER| \Rightarrow GWN \overset{ID}{\longleftrightarrow} USER$ The user has complete jurisdiction over the state $|\psi_{USER}\rangle = f(ID_{USER} \| Puk)$ generated by the user. The state is shared between the User and GWN by utilizing Pauli gates.

- H15: $SN| \equiv \#(sk)$: Sensor Node believes the fresh secret key is generated.

- H16: $SN \overset{sk}{\longleftrightarrow} GWN| \equiv (SN \overset{sk}{\longleftrightarrow} GWN)_{Bs'GS}$:sk is shared between SN and GWN.GWN believes the sk is generated using a basis between SN and GWN.

- H17: $GWN| \equiv GWN \overset{sk}{\longleftrightarrow} SN| \Rightarrow (GWN \overset{sk}{\longleftrightarrow} SN)_{Bs'GS}$: GWN believe that the secret key is communicated between GWN and SN, and SN has jurisdiction over the basis state used for generating the sk.

- H18: $GWN| \equiv SN| \Rightarrow \#(sk)$: GWN believes SN has jurisdiction over generating the fresh sk.

- H19: $(GWN \overset{ID}{\longleftrightarrow} SN)_H| \Rightarrow GWN \overset{ID}{\longleftrightarrow} SN$: GWN sends the encoded state to SN, which contains the User ID and sends measurement Basis.

- H20: $GWN| \equiv USER| \Rightarrow USER \xleftrightarrow{ID_{QGC}} GWN$: User has jurisdiction over the user id shared by User with GWN using QGC.

- H21: $GWN \xleftrightarrow{(\uparrow\downarrow)_H} SN| \Rightarrow SN \xleftrightarrow{(\uparrow\downarrow)_H} GWN$. SN ID is exchanged using H-Basis by SN; therefore, SN has jurisdiction over the SN ID communicated with GWN.

- H22: $USER| \equiv GWN| \equiv SN(GWN \xleftrightarrow{(\uparrow\downarrow)_H} SN)$. The user believes in GWN, and GWN believes in SN, over the statement that corrected state (User ID)obtained by applying Pauli Z-Gate on SN state.

- H23: $USER| \equiv SN| \Rightarrow (SN \overset{ID}{\longleftrightarrow} USER)$: User believes in SN, over the statement that they both share the same identity by evaluating: $|\psi_{SN2}\rangle$=$f(ID_{GWN} \| ID_{QSN} \| ID_{USER})$.

- H24:$USER| \equiv | \Rightarrow (SN \overset{ID}{\longleftrightarrow} USER)$: User believes the statement that they both share the same id by evaluating $|\psi_{US}\rangle = f(ID_{USER}||ID_{QSN})$.

- H25: $SN| \equiv USER| \Rightarrow (USER \overset{ID}{\longleftrightarrow} SN)$ SN believe user, that the user has jurisdiction over the statement that both the User and Sensor share the same ID by evaluating $|\phi^{(i)}\rangle_{U2}$.

- H26: $USER| \equiv SN(SN \overset{sk}{\leftrightarrow} GWN)$: User believes SN, over the statement that the sk is generated and shared between SN and GWN.

- H27: $USER| \equiv SN| \equiv GWN(SN \overset{ID}{\longleftrightarrow} GWN)$ User believes SN and SN believe GWN that based on GWN node shared (H)basis, SN correct its state; therefore, both SN and GWN share the same ID.

- H28: $USER| \equiv GWN_- > USER$: $C_2'(x)$ User believes that GWN measures its qubits and sends measure qubits to USER.

- H29:$SN| \equiv GWN| \Rightarrow (GWN \overset{ID}{\longleftrightarrow} USER)$: SN believes GWN over the statement that GWN has a Jurisdiction, that both GWN and USER share the same ID registered by User.

- H30: $USER| \equiv GWN| \Rightarrow (USER \overset{ID}{\longleftrightarrow} GWN)$: The user believes GWN and GWN have Jurisdiction that both USER and GWN share the same ID.

- H31: $SN| \equiv GWN| \equiv USER| \Rightarrow (GWN \overset{sk}{\leftrightarrow} USER)$ SN believes GWN and GWN believe user, that the user has jurisdiction over the shared key, sk between GWN and the User.

- H32: $GWN| \equiv USER : (GWN \overset{sk}{\leftrightarrow} USER), (GWN \overset{\uparrow\downarrow}{\leftrightarrow} SN)_H$,
$(USER \overset{\uparrow\downarrow}{\leftrightarrow} SN)_Z$:By evaluating $\{|\psi^{(i)}_{UIN}\rangle|\psi'^{(i)}_{UIN}\rangle$, GWN believe User over the statement that both GWN and User share the same id, GWN retrieves user information and shares it with GWN.

- H33: $GWN| \equiv SN : (SN \overset{sk}{\leftrightarrow} GWN), (SN \xleftrightarrow{(\uparrow\downarrow)} GWN)_H$, $(SN \overset{\uparrow\downarrow}{\leftrightarrow} GWN)_Z$: By evaluating $\{|\psi_{SN1}\rangle|\psi'_{SN1}\rangle\}$ GWN believe SN that they both share the same id and basis is shared between legitimate SN and GWN.
  Now, the sequences of main proof to achieve the goal stated above are provided below:
  From M1, it is easy to get the statement:

S1: $GWN \lhd (USER \overset{sk}{\leftrightarrow} GWN)_{Bs'UG}, (USER \xleftrightarrow{ID_{QGC}} GWN)_{|\phi^{(i)}\rangle_{U2}}$

On the basis of H5, S1, Message –Meaning rule (A1), we get:

S2: $USER| \equiv GWN(USER \overset{sk}{\leftrightarrow} GWN)_{Bs'U}$

On the basis of H6, S2, Jurisdiction rule (A3), we get:

S3: $GWN| \equiv USER| \Rightarrow (\leftrightarrow \nearrow \updownarrow \nwarrow)_{Bs'U}.$

On the basis of H7, S3, Nonce verification rule (A2), we get:

S4: $USER| \equiv (GWN \overset{sk}{\leftrightarrow} USER)$ **[Goal 1]**

On the basis of H12, S4, Freshness rule (A4), we get:

S5: $GWN| \equiv USER| \sim (GWN \overset{sk}{\leftrightarrow} USER)$

On the basis of H9, S5, Shared key rule (A5), we get:

S6: $USER| \equiv GWN| \equiv (GWN \overset{sk}{\leftrightarrow} USER)$ **[Goal 2]**

On the basis of H14, S6, Message –Meaning rule (A1) ,we get :

S7: $USER| \equiv GWN| \equiv ((USER \overset{sk}{\leftrightarrow} GWN), (GWN \overset{ID}{\longleftrightarrow} USER)_{|\phi^{(i)}_{U2}\rangle})$

On the basis of H20, S7, Believe rule (A6), we get:

S8: $GWN| \equiv (USER \overset{ID}{\longleftrightarrow} GWN)$ **[Goal 6]**

From M2, it is easy to get the statement:

S9:SN $\lhd (SN \overset{ID}{\longleftrightarrow} GWN)_{|\phi^{(i)}\rangle_{U2}}, (SN \overset{sk}{\leftrightarrow} GWN)_{Bs'SG}$

From H19, S9, and Believe rule (A6), we get:

S10:SN $| \equiv GWN(H, SN \overset{ID}{\longleftrightarrow} GWN)$

From H22, S10, Message meaning rule (A1) we get:

S11: $GWN| \equiv (Z, SN \overset{ID}{\longleftrightarrow} GWN)$ **[Goal 3]**

From H16, S11 Believe rule (A3), we get:

S12: $SN| \equiv GWN| \equiv (GWN \overset{sk}{\leftrightarrow} SN)$ **[Goal 4]**

From message 3, we get the statement:

S13: $USER \lhd (SN \overset{ID}{\longleftrightarrow} USER)_{|\psi_{SN2}\rangle}, (USER \overset{sk}{\leftrightarrow} GWN)_{Bs'UG}$

From H25, S13, Jurisdiction rule (A3), we get:

S14: $USER| \equiv SN| \sim (SN \overset{ID}{\longleftrightarrow} GWN)_{|\psi_{SN2}\rangle}$

From H27, S14, Believe rule (A6) we get:

S15: $USER| \equiv SN| \equiv (USER \overset{ID}{\longleftrightarrow} SN)$ **[Goal 5]**

From H13, S15, Message –Meaning rule (A1), we get:

S16: $SN| \equiv GWN| \equiv USER(GWN \overset{sk}{\leftrightarrow} USER)$

From H20, S16, Believe rule (A6), we get:

S17:$SN| \equiv USER| \equiv (USER \overset{ID}{\longleftrightarrow} SN)$ **[Goal 7]**

After achieving Goals 1, 4, and 7, we can ensure that the QAKA protocol achieved the Secure Key agreement, MA, the Shared Key, sk, and the user and SN's identity.

3.3.2 Security verification using Random Oracle Model(ROM)

For the proposed protocol, we present the formal security analysis using the ROM.

Theorem 1: Under the assumption that OWF f(.) works like a random oracle, even in case the user lost his QGC, against an adversary $\bar{A}$ for ID_{USER} and shared key (sk) of the user, the QAKA protocol is proved secure.

Proof: Here, for proof, we assume an adversary $\bar{A}$, who can obtain the user credentials such as (ID_{USER}, sk) Quantum Password(QP) is issued to the user and QGC as the adversary $\bar{A}$ by performing a power analysis attack can extract the information[102]. In the QAKA protocol, the reveal oracle is used by the adversary $\bar{A}$ to perform the experimental algorithm as represented in Algorithm 1 $EP1^{QAKA}_{HASH,\bar{A}}$ The success probability Pr(.) for the $EP1^{QAKA}_{HASH,\bar{A}}$is defined by $SUCCESS1^{QAKA}_{HASH,\bar{A}}$=$|Pr[EP1^{QAKA}_{HASH,\bar{A}} = 1] - 1$. The advantage function for this experiment is defined by $ADVT1^{QAKA}_{HASH,\bar{A}}$ $(T_i, Q_i) = max_A$ $\{Success1^{QAKA}_{HASH,\bar{A}}\}$, where the maximum is decided by the two factors: execution time (T_i), and number of queries derived from Reveal Oracle (Q_i).Our scheme is secure against the adversary $\bar{A}$, to obtain ID_{USER},sk, the identity of Gateway (GW), puk and prk if $ADVT1^{QAKA}_{HASH,\bar{A}}$ $\leq \in, \forall \in > 0$.As represented in Algorithm 1 adversary $\bar{A}$, can attain the credentials of the user if it can invert the OWF f(.) function. However, hash functions are irreversible and $ADVT1^{QAKA}_{HASH,\bar{A}}$ $\leq \in$ for any sufficiently small $\in > 0$.Similarly, if the adversary $\bar{A}$, may not be able to generate the shared key (sk), as to generate the sk random basis is shared over the Quantum secure channel, which is impossible for the adversary to intercept with acceptable probability. As a result, QAKA is secure against an adversary $\bar{A}$ to obtain ID_{USER},sk, the identity of Gateway (GW), Public Key (puk) and Private Key (prk).

Algorithm 1 $EP1^{QAKA}_{HASH,\bar{A}}$

```
Extract information stored in $\{Puk, Prk, sk, |\psi^{(i)}_{UIN}\rangle\}$ QGC
Call reveal oracle. Let $(ID_{USER}', Puk') \leftarrow Reveal1(A_i')$
Call reveal oracle Let $(ID_{USER}', Prk') \leftarrow Reveal2(B_i')$
Call reveal oracle. Let $(ID_{USER}', sk') \leftarrow$ Reveal3 $(|\psi^{(i)}_{UIN}{}'\rangle)$
Compute $A_i'=f(ID_{USER}' \| Puk')$
If $(A_i'=A_i)$ then
Accept user-id
Compute $B_i' = f(ID_{USER}' \| Prk')$
If $(B_i'=B_i)$ then
Generate shared key,$sk'$
Compute $|\psi^{(i)}_{UIN}{}'\rangle$ = f$(ID_{USER}' \| sk')$
If $(|\psi^{(i)}_{UIN}{}'\rangle = |\psi^{(i)}_{UIN}\rangle)$
Accept user request
Return 1(Success)
Else
            Return 0
End If
Else
            Return 0
End If
Else
            Return 0
End If
```

Theorem 2: Under the assumption that OWF f(.) behaves like a random oracle, QAKA protocol for the user is provably secure against an adversary $\bar{A}$ for (ID_{USER}, QP), shared key (sk) and QGC.

Proof: To prove this theorem, we assume that there is an adversary who has the capability to obtain the user credentials as User ID (ID_{USER}), Public Key (Puk) of the user, Quantum Password (QP) shared with the user, shared key (sk), the identity of Gateway Node and the identity of QGC. For generating all this information Adversary $\bar{A}$ is required to execute $EP2^{QAKA}_{HASH,\bar{A}}$ which is depicted in Algorithm 2. The probability (Pr) of success can be considered as $SUCCESS2^{QAKA}_{HASH,\bar{A}}$=$|Pr[EP2^{QAKA}_{HASH,\bar{A}} = 1] - 1$.The advantage function for this experiment is defined by $ADVT2^{QAKA}_{HASH,\bar{A}}$ (T_i, Q_i) = max_A $\{Success2^{QAKA}_{HASH,\bar{A}}\}$, where the maximum is decided by the two factors: processing duration (T_i), and the quantity of queries obtained from the Reveal Oracle (Q_i).QAKA protocol is secure against the adversary $\bar{A}$, to drive User ID (ID_{USER}), Public Key (Puk) of the user, Quantum Password (QP) sent to the user communicating device, shared key (sk), the identity of Gateway Node and identity of Quantum Green Card (QGC). $ADVT2^{QAKA}_{HASH,\bar{A}}$ $\leq\in$,$\forall$ $\in>$ 0.In the experiment represented in Algorithm 2, adversaries can obtain the user credentials if they can invert the OWF f(.)function. However, hash functions are irreversible and $ADVT2^{QAKA}_{HASH,\bar{A}}$ $\leq\in$ for any sufficiently small $\in>$ 0.Similarly, if the adversary $\bar{A}$, may not be able to generate the QP, as to generate the QP the user needs to securely generate sk with GWN which is impossible as the information is communicated using a random basis. As a result, QAKA is secure against an adversary $\bar{A}$ to obtain the user identity (ID_{USER}), Public Key(puk), Quantum Password (QP), shared key (sk), identity of Gateway Node (ID_{GWN}) and identity of QGC.

Algorithm 2 $EP2^{QAKA}_{HASH,\bar{A}}$

```
During the login phase, the adversary $\bar{A}$ eavesdrop the information $\{|\psi^{(i)}_{UIN}\rangle, |\psi_{USER}\rangle, |\phi_{QP}\rangle\}$
Call reveal oracle. Let $(ID_{USER}', sk')$← Reveal1 ($|\psi^{(i)}_{UIN}{}'\rangle$)
Call reveal oracle. Let $(ID_{USER}', Puk')$ ← Reveal2 ($|\psi^{(i)}_{USER}{}'\rangle$)
Compute $|\psi^{(i)}_{UIN}{}'\rangle$ =$f(ID_{USER}'\|sk')$
If ($|\psi^{(i)}_{UIN}{}'\rangle = |\psi^{(i)}_{UIN}\rangle$) then
Allow users to share secrets.
Compute $|\psi^{(i)}_{USER}{}'\rangle = f(ID_{USER}'\|Puk')$.
If ($|\psi^{(i)}_{USER}{}'\rangle = |\psi^{(i)}_{USER}\rangle$)
Allow Gateway to generate $\{|\phi_{QP}{}'\rangle\}$.
If ($|\phi_{QP}{}'\rangle = |\phi_{QP}\rangle$).
Accept user requests
Return 1(Success)
Else
            **Return 0**
End If
Else
            **Return 0**
End If
Else
            **Return 0**
End If
```

3.3.3 Simulation of QAKA Protocol Using AVISPA Tool

This section will simulate the proposed QAKA protocol using the widely accepted AVISPA (SPAN) tool for formal security verification. We first present the proposed protocol's HLPSL specification and then simulate using OFMC and CL-AtSe backends.

3.3.3.1 HLPSL specification

In the proposed QAKA protocol: the user, GW node and SN are represented as the user, gw and ss, respectively. These are the considered three basic roles for HLPSL specification. The session and environment are the other two roles. In HLPSL, the user's role is represented in Figure 3.9. In the registration phase, the user starts at State =0 and then receives the signal by transitioning from State =0 → $State' = 1$.The user generates A_i' and witness (GWN, Ui, gw_u_ai, A_i'), which means A_i' is a fresh value generated Ui intended for GWN. The statement secret $(\{A_i'\}, sec\_ai, \{U_i, GWN\})$ means that A_i' is secret and kept by Ui. It is characterized by *protocol_id sec_ai*. After calculating A_i',U_i shares the registration request with GWN. In State =1,U_i receives$\{B_i{}' = H(UID.Ai')\}$,by RCV()operation. After State =1,the next state transition is State'=2;GWN requests U_i for considering the value $\{B_i'\}$ computed by GWN for U_i.The operation is performed using request $(U_i, GWN, u\_gw\_bi, B_i{}')$.The user receives$\{SK'\}$ from GWN, and GWN requests to Ui undertake the value $\{SK'\}$.In transition 7, the user generates a new value SKU' using a new() operation and computes $UIN' := H(UID.SKU')$.

The statement secret $(\{UIN'\}, sec_{uin}, \{Ui, GWN\})$ means that UIN' is characterized by protocol_id sec_uin. Users also send UIN' using the SND() operation. It also computes USR':= H(UID. PUKUi') and sends UIN', USR' using SND() operation to GWN for authentication purposes.

The user uses the uses statement, witness $(GWN, Ui, gw\_u\_uin, UIN')$ and $(GWN, Ui, gw\_u\_usr, USR')$ means Ui has generated fresh value UIN' and USR' intended for GWN. After registration, in transition 8, for legitimate login, the user receives{QP'} from GWN for a particular session. After successful authentication from GWN, it receives {SN2'} from the sensor node. The user also computes $UA' := H(UID.SN2')$ and SN requests to Ui for the undertaking of the value $\{Ui, SN, u\_sn\_sn2, SN2'\}$. The statement secret $(\{UA'\}, sec\_ua, Ui, SN)$ means that UA' is characterized by protocol_id sec_uin.

Similarly, Figure 3.10 and Figure 3.11 specify the role of GWN and SN, respectively. The roles of the session, environment, and goal are described in Figure 3.12 and Figure 3.13. In this 10 secrecy and 13 authentication goals are specified to be verified.

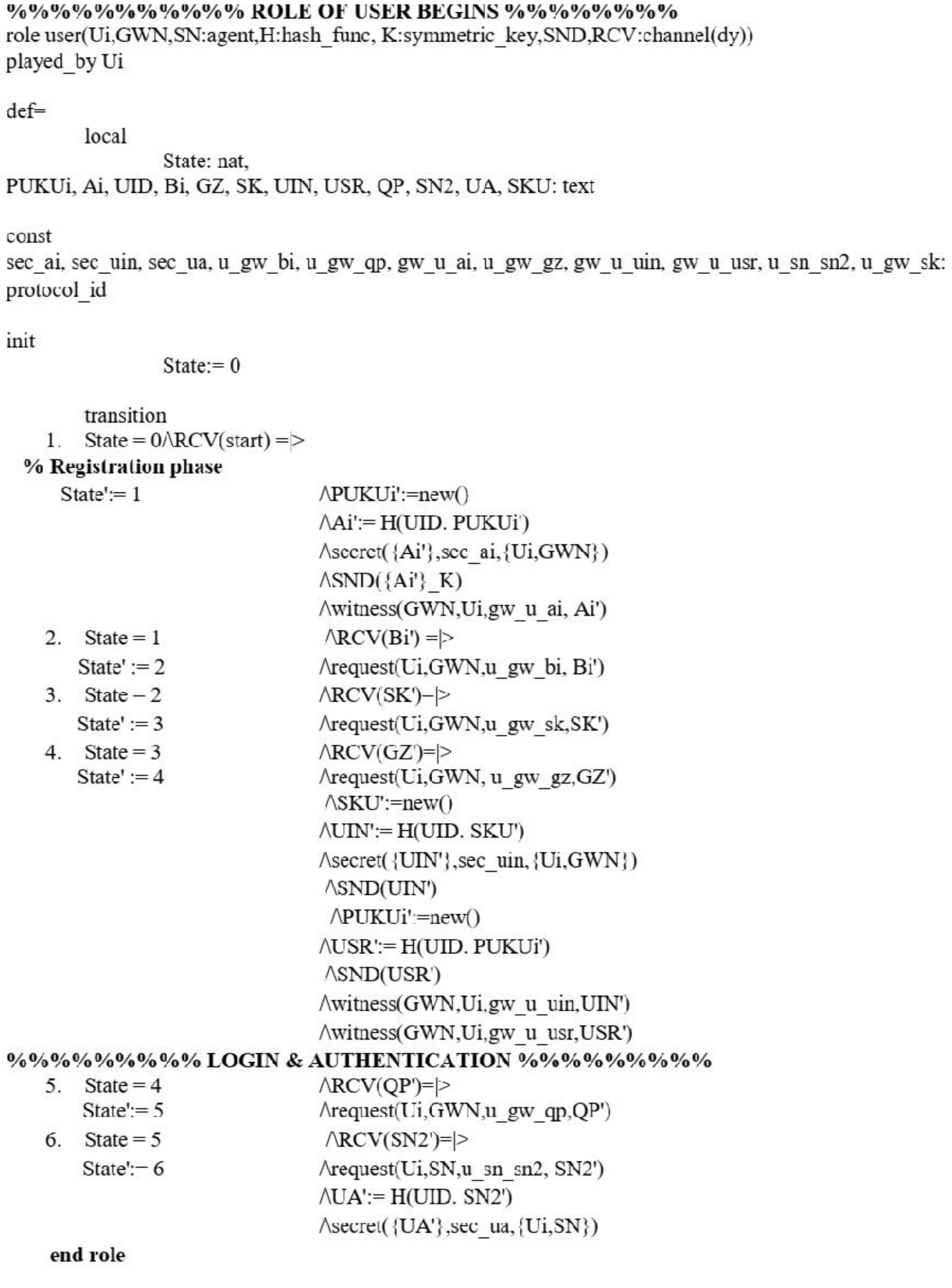
3.3.3.2 Simulation of QAKA protocol

The simulation results for both the OFMC and CL-AtSe back-ends are depicted in Figure 3.14, illustrating the safety and security of the QAKA protocol.

3.3.4 Informal Security Analysis

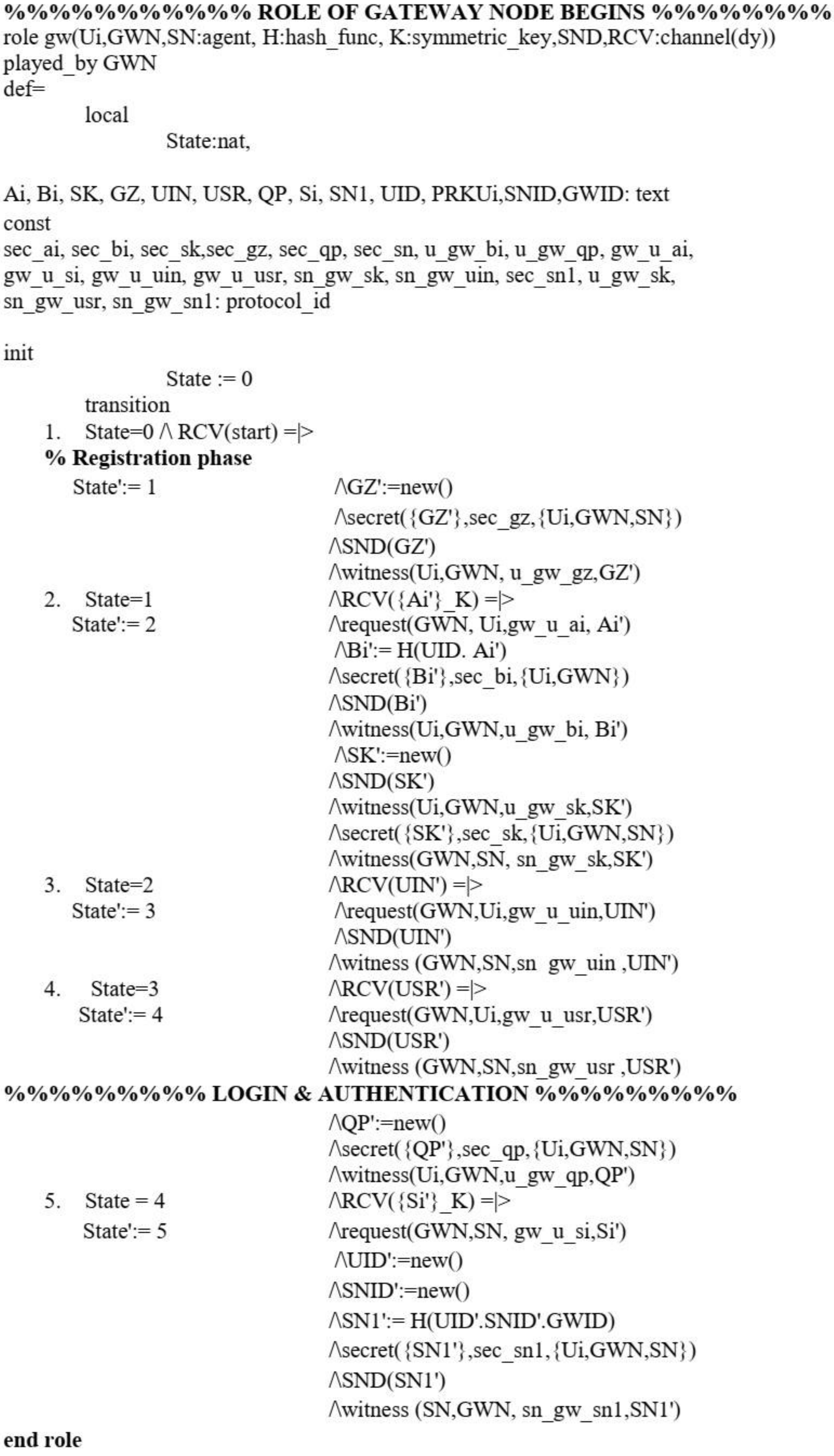
In this section, we also proved the correctness of the proposed QAKA scheme. Here, we discussed the theorems with their proof to prove the security of the proposed protocol.

- **Correctness**:
  Theorem 1: By considering all entities entangled, follow the Quantum Authentication and Key Agreement (QAKA) Protocol. Equation (7) holds:



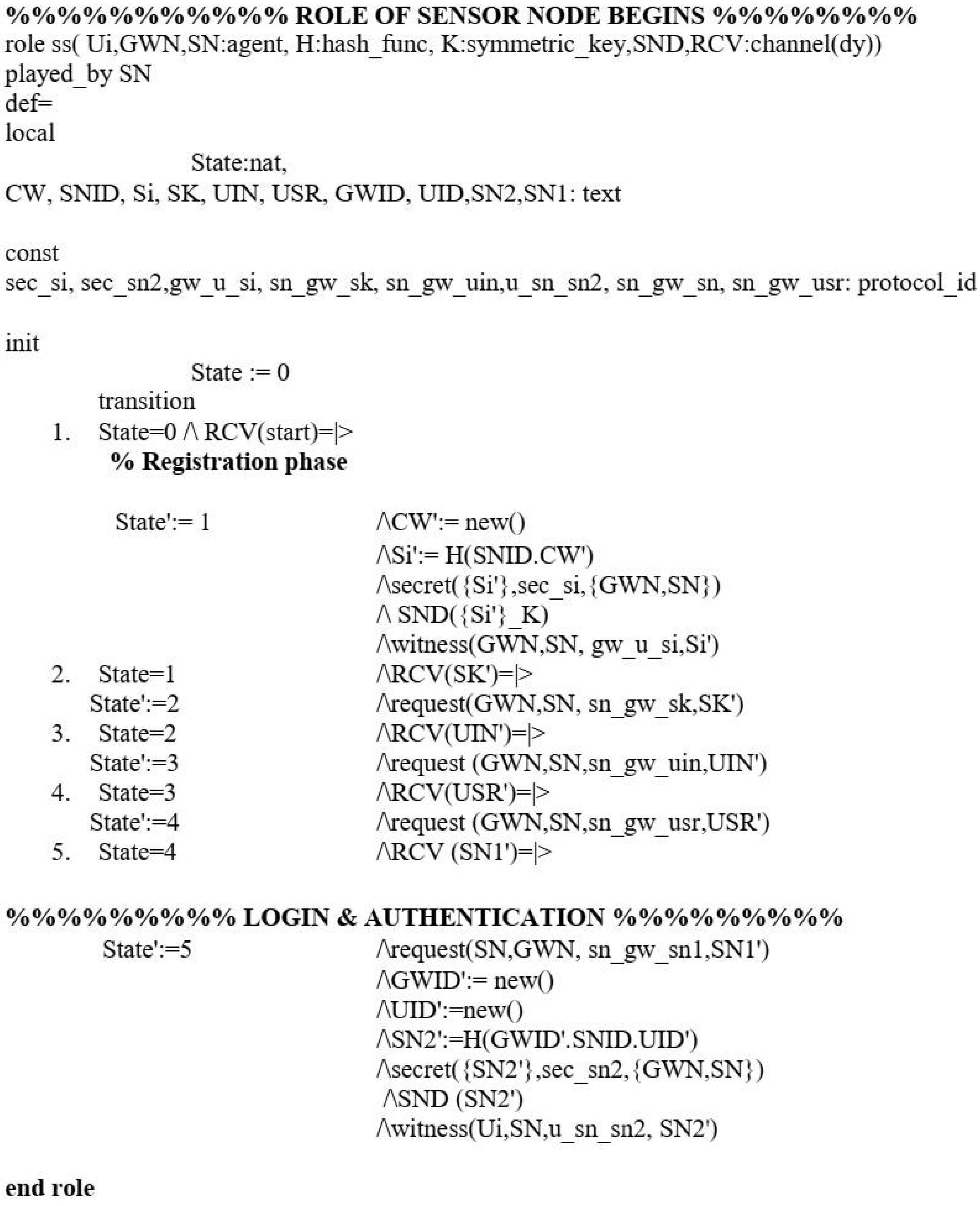
```
%%%%%%%%%%%% ROLE OF USER BEGINS %%%%%%%%
role user(Ui,GWN,SN:agent,H:hash_func, K:symmetric_key,SND,RCV:channel(dy))
played_by Ui

def=
        local
                State: nat,
PUKUi, Ai, UID, Bi, GZ, SK, UIN, USR, QP, SN2, UA, SKU: text

const
sec_ai, sec_uin, sec_ua, u_gw_bi, u_gw_qp, gw_u_ai, u_gw_gz, gw_u_uin, gw_u_usr, u_sn_sn2, u_gw_sk:
protocol_id

init
                State:= 0

        transition
    1.  State = 0/\RCV(start) =|>
 % Registration phase
      State':= 1                /\PUKUi':=new()
                                /\Ai':= H(UID. PUKUi')
                                /\secret({Ai'},sec_ai,{Ui,GWN})
                                /\SND({Ai'}_K)
                                /\witness(GWN,Ui,gw_u_ai, Ai')
    2.  State = 1                /\RCV(Bi') =|>
      State' := 2               /\request(Ui,GWN,u_gw_bi, Bi')
    3.  State – 2               /\RCV(SK')–|>
      State' := 3               /\request(Ui,GWN,u_gw_sk,SK')
    4.  State = 3               /\RCV(GZ')=|>
      State' := 4               /\request(Ui,GWN, u_gw_gz,GZ')
                                 /\SKU':=new()
                                /\UIN':= H(UID. SKU')
                                /\secret({UIN'},sec_uin,{Ui,GWN})
                                 /\SND(UIN')
                                  /\PUKUi':=new()
                                /\USR':= H(UID. PUKUi')
                                 /\SND(USR')
                                /\witness(GWN,Ui,gw_u_uin,UIN')
                                /\witness(GWN,Ui,gw_u_usr,USR')
%%%%%%%%%% LOGIN & AUTHENTICATION %%%%%%%%%
    5.  State = 4               /\RCV(QP')=|>
       State':= 5               /\request(Ui,GWN,u_gw_qp,QP')
    6.  State = 5                /\RCV(SN2')=|>
       State':– 6               /\request(Ui,SN,u_sn_sn2, SN2')
                                /\UA':= H(UID. SN2')
                                /\secret({UA'},sec_ua,{Ui,SN})

    end role
```

Figure 3.9: User: HLPSL code for QAKA protocol.



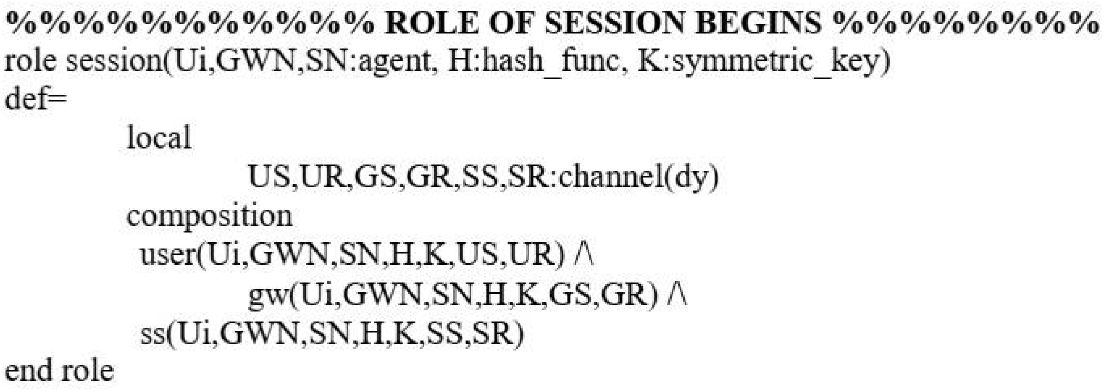
```
%%%%%%%%%%%%% ROLE OF GATEWAY NODE BEGINS %%%%%%%%%
role gw(Ui,GWN,SN:agent, H:hash_func, K:symmetric_key,SND,RCV:channel(dy))
played_by GWN
def=
          local
                    State:nat,

Ai, Bi, SK, GZ, UIN, USR, QP, Si, SN1, UID, PRKUi,SNID,GWID: text
const
sec_ai, sec_bi, sec_sk,sec_gz, sec_qp, sec_sn, u_gw_bi, u_gw_qp, gw_u_ai,
gw_u_si, gw_u_uin, gw_u_usr, sn_gw_sk, sn_gw_uin, sec_sn1, u_gw_sk,
sn_gw_usr, sn_gw_sn1: protocol_id

init
                    State := 0
          transition
     1.   State=0 /\ RCV(start) =|>
     % Registration phase
         State':= 1                 /\GZ':=new()
                                    /\secret({GZ'},sec_gz,{Ui,GWN,SN})
                                   /\SND(GZ')
                                   /\witness(Ui,GWN, u_gw_gz,GZ')
     2.   State=1                  /\RCV({Ai'}_K) =|>
         State':= 2                /\request(GWN, Ui,gw_u_ai, Ai')
                                    /\Bi':= H(UID. Ai')
                                   /\secret({Bi'},sec_bi,{Ui,GWN})
                                   /\SND(Bi')
                                   /\witness(Ui,GWN,u_gw_bi, Bi')
                                    /\SK':=new()
                                   /\SND(SK')
                                   /\witness(Ui,GWN,u_gw_sk,SK')
                                   /\secret({SK'},sec_sk,{Ui,GWN,SN})
                                   /\witness(GWN,SN, sn_gw_sk,SK')
     3.   State=2                  /\RCV(UIN') =|>
         State':= 3                 /\request(GWN,Ui,gw_u_uin,UIN')
                                    /\SND(UIN')
                                   /\witness (GWN,SN,sn  gw_uin ,UIN')
     4.    State=3                 /\RCV(USR') =|>
          State':= 4               /\request(GWN,Ui,gw_u_usr,USR')
                                   /\SND(USR')
                                   /\witness (GWN,SN,sn_gw_usr ,USR')
%%%%%%%%%% LOGIN & AUTHENTICATION %%%%%%%%%
                                   /\QP':=new()
                                   /\secret({QP'},sec_qp,{Ui,GWN,SN})
                                   /\witness(Ui,GWN,u_gw_qp,QP')
     5.   State = 4                /\RCV({Si'}_K) =|>
          State':= 5               /\request(GWN,SN, gw_u_si,Si')
                                    /\UID':=new()
                                   /\SNID':=new()
                                   /\SN1':= H(UID'.SNID'.GWID)
                                   /\secret({SN1'},sec_sn1,{Ui,GWN,SN})
                                   /\SND(SN1')
                                   /\witness (SN,GWN, sn_gw_sn1,SN1')
end role
```

Figure 3.10: GW: HLPSL code for QAKA protocol.



```
%%%%%%%%%%%%% ROLE OF SENSOR NODE BEGINS %%%%%%%%%
role ss( Ui,GWN,SN:agent, H:hash_func, K:symmetric_key,SND,RCV:channel(dy))
played_by SN
def=
local
                State:nat,
CW, SNID, Si, SK, UIN, USR, GWID, UID,SN2,SN1: text

const
sec_si, sec_sn2,gw_u_si, sn_gw_sk, sn_gw_uin,u_sn_sn2, sn_gw_sn, sn_gw_usr: protocol_id

init
                State := 0
        transition
    1.  State=0 /\ RCV(start)=|>
         % Registration phase

         State':= 1                /\CW':= new()
                                   /\Si':= H(SNID.CW')
                                   /\secret({Si'},sec_si,{GWN,SN})
                                   /\ SND({Si'}_K)
                                   /\witness(GWN,SN, gw_u_si,Si')
    2.  State=1                    /\RCV(SK')=|>
       State':=2                   /\request(GWN,SN, sn_gw_sk,SK')
    3.  State=2                    /\RCV(UIN')=|>
       State':=3                   /\request (GWN,SN,sn_gw_uin,UIN')
    4.  State=3                    /\RCV(USR')=|>
       State':=4                   /\request (GWN,SN,sn_gw_usr,USR')
    5.  State=4                    /\RCV (SN1')=|>

%%%%%%%%%% LOGIN & AUTHENTICATION %%%%%%%%%%
        State':=5                  /\request(SN,GWN, sn_gw_sn1,SN1')
                                   /\GWID':= new()
                                   /\UID':=new()
                                   /\SN2':=H(GWID'.SNID.UID')
                                   /\secret({SN2'},sec_sn2,{GWN,SN})
                                    /\SND (SN2')
                                   /\witness(Ui,SN,u_sn_sn2, SN2')

end role
```

Figure 3.11: SN: HLPSL code for QAKA protocol.



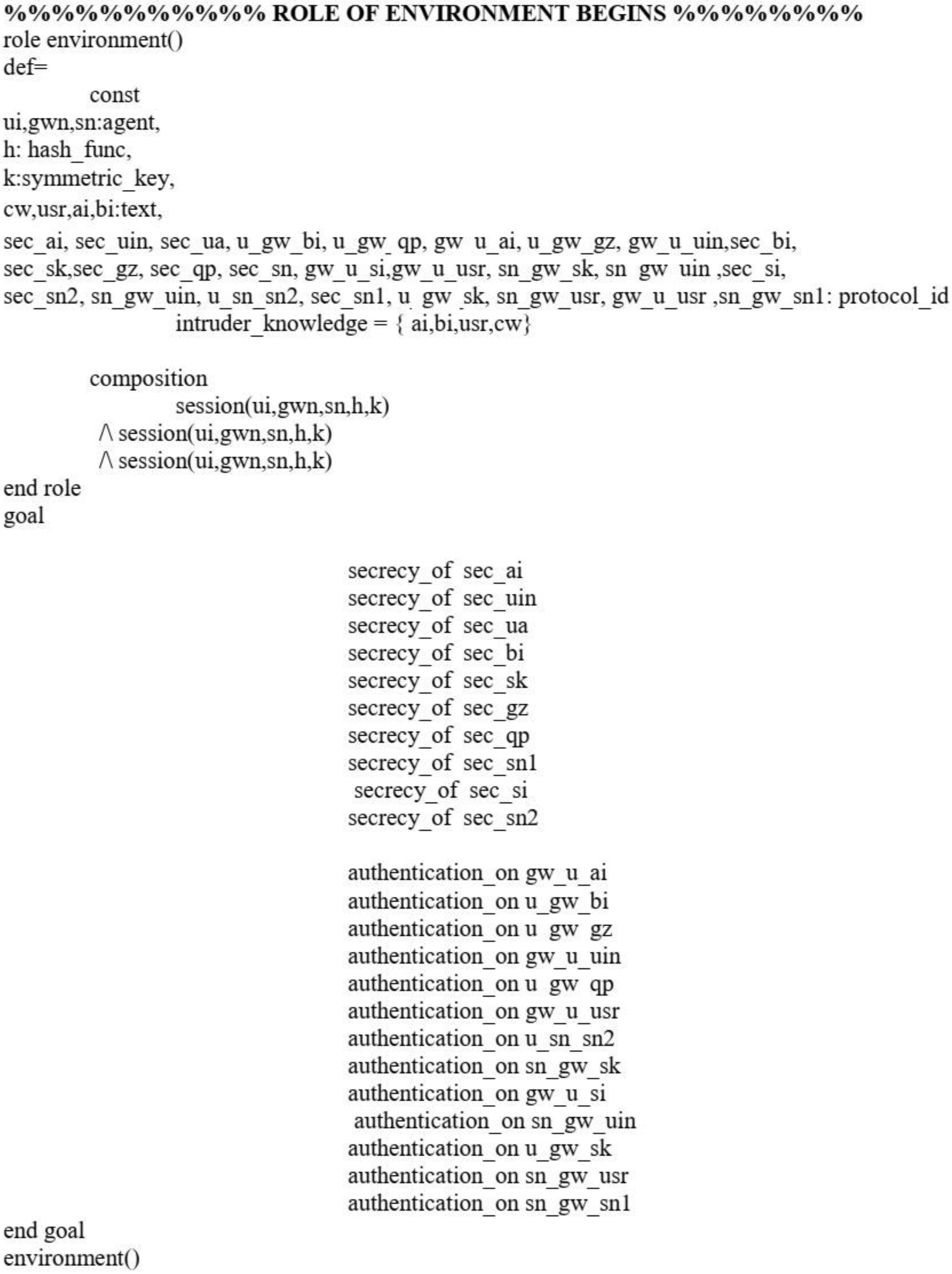
```
%%%%%%%%%%%% ROLE OF SESSION BEGINS %%%%%%%%%
role session(Ui,GWN,SN:agent, H:hash_func, K:symmetric_key)
def=
        local
                US,UR,GS,GR,SS,SR:channel(dy)
        composition
         user(Ui,GWN,SN,H,K,US,UR) /\
                gw(Ui,GWN,SN,H,K,GS,GR) /\
         ss(Ui,GWN,SN,H,K,SS,SR)
end role
```

Figure 3.12: Session role: HLPSL code for QAKA protocol.

Proof: The correctness of the protocol can be measured by inspecting the entity's user, GWN and QSN. In addition, we also inspect Adversary A, whose presence is inaudible on the network while entities are involved in the communication process. However, if there is no intervention, GWN successfully processes the secret key with the user and QSN. Using the QKD algorithm, even if A can effortlessly forge user credentials, it would still require a shared key, sk corresponding to the user id. In addition, in our protocol, the QGC stores user credentials, as Quantum states, that are provided to legitimate users. The scheme does make it impossible for adversaries to forge quantum states.
Also, quantum entanglement is monogamous for maximally entangled (GHZ) states. The GHZ states are shared with only authenticated GWN, its trusted user, and QSN. Therefore, A does not have the required pair of these maximally entangled particles. Hence, it would be unfeasible for an adversary to create a quantum state $\{|\phi^{(i)}\rangle_{GHZ}\}_{i=1:m}$ as GWN would only verify that state.

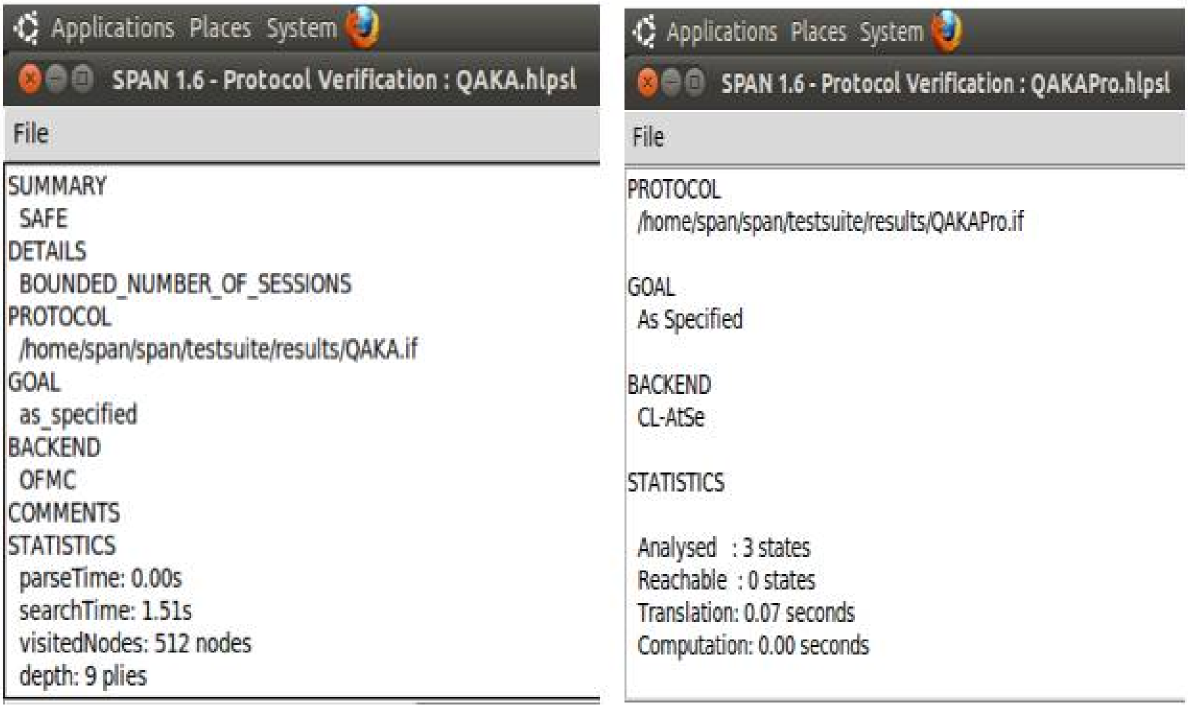
- **Security against repudiation:**
  Suppose user A repudiates earlier access to information from the QSN. The QSN will resort to GWN. The GWN verifies the state presented by the user, $|\psi^{(i)}_{UIN}\rangle$ by computing $|\psi'^{(i)}_{UIN}\rangle$. However, GWN asks the A's capacity to repudiate the login by presenting the user as a GHZ particle. The user's impossibility of producing the Quantum states concludes that the attacker has forged user credentials.

- **Impossibility of cloning:**
  For contradiction, QGC containing personal user credentials is in its quantum memory. Let $\{X_1, X_2, X_3.....X_n\}$ be the frequency of occurrences attacker 'A' is allowed to run an experiment to copy the unknown quantum state$\{Q_1, Q_2, Q_3....Q_n\}$ containing user credentials. An adversary 'A' interrupts the quantum state, Q. Let $Q \leftarrow Exp_{(A,Q)}(1^z)$ denote the experiment. The adversary runs the experiment to generate the user's secret information by applying Quantum operations using ancilla qubits as in Eq.3.6:
  $$(stat.) \leftarrow Gen(1^z) \tag{3.6}$$
  Where states are the total quantum states prepared by the GEN algorithm, and Z is the security measurement parameter. Adversary A allowed experimenting by



```
%%%%%%%%%%%% ROLE OF ENVIRONMENT BEGINS %%%%%%%%%
role environment()
def=
          const
ui,gwn,sn:agent,
h: hash_func,
k:symmetric_key,
cw,usr,ai,bi:text,
sec_ai, sec_uin, sec_ua, u_gw_bi, u_gw_ qp, gw  u_ai, u_gw_gz, gw_u_uin,sec_bi,
sec_sk,sec_gz, sec_qp, sec_sn, gw_u_si,gw_u_usr, sn_gw_sk, sn  gw  uin ,sec_si,
sec_sn2, sn_gw_uin, u_sn_sn2, sec_sn1, u  gw  sk, sn_gw_usr, gw_u_usr ,sn_gw_sn1: protocol_id
                    intruder_knowledge = { ai,bi,usr,cw}

          composition
                    session(ui,gwn,sn,h,k)
           /\ session(ui,gwn,sn,h,k)
           /\ session(ui,gwn,sn,h,k)
end role
goal

                                        secrecy_of  sec_ai
                                        secrecy_of  sec_uin
                                        secrecy_of  sec_ua
                                        secrecy_of  sec_bi
                                        secrecy_of  sec_sk
                                        secrecy_of  sec_gz
                                        secrecy_of  sec_qp
                                        secrecy_of  sec_sn1
                                         secrecy_of  sec_si
                                        secrecy_of  sec_sn2

                                        authentication_on gw_u_ai
                                        authentication_on u_gw_bi
                                        authentication_on u  gw  gz
                                        authentication_on gw_u_uin
                                        authentication_on u  gw  qp
                                        authentication_on gw_u_usr
                                        authentication_on u_sn_sn2
                                        authentication_on sn_gw_sk
                                        authentication_on gw_u_si
                                         authentication_on sn_gw_uin
                                        authentication_on u_gw_sk
                                        authentication_on sn_gw_usr
                                        authentication_on sn_gw_sn1
end goal
environment()
```

Figure 3.13: Environment role: HLPSL code for QAKA protocol.


Applications Places System
SPAN 1.6 - Protocol Verification : QAKA.hlpsl
File

```
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/QAKA.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 1.51s
  visitedNodes: 512 nodes
  depth: 9 plies
```

Applications Places System
SPAN 1.6 - Protocol Verification : QAKAPro.hlpsl
File

```
PROTOCOL
 /home/span/span/testsuite/results/QAKAPro.if

GOAL
 As Specified

BACKEND
 CL-AtSe

STATISTICS

 Analysed   : 3 states
 Reachable  : 0 states
 Translation: 0.07 seconds
 Computation: 0.00 seconds
```

Figure 3.14: QAKA Simulation: OFMC and CL-AtSe Backends.

running queries to QGC Oracle to generate user id and puk as in Eq3.7:

$$Let, Q \leftarrow A^{QGC}(id, puk) \tag{3.7}$$

To verify the state, let the event be in Eq3.8:

$$(verify(Q') = 1) \wedge Q' \qquad Q_1, Q_2, Q_n \tag{3.8}$$

We also consider the state Q unconditionally secure; WIN A, Q for an adversary to be negligible even with unbounded resources and computing power due to the No-Cloning principle. Therefore, physics laws limit A. According to quantum physics law, generating a clone of state $|\psi\rangle$ is impracticable.

3.4 Results and Discussion

In this section, we first discuss the technical challenges of the proposed scheme for resource-constrained IoT networks. Next, we provide a comparative analysis of the proposed protocol. Lastly, we compare the security characteristics of the proposed scheme with those of other authentication protocols.

3.4.1 Technical Challenges

However, Quantum-based solutions provide many advantages over classical cryptographic primitives, but existing schemes cannot be easily adapted to Quantum-based solutions due to certain technical challenges. We briefly explain those as:

- **Classical primitives:**
  The existing authentication techniques are based on classical mathematical primitives such as RSA. These are designed to encounter classical attacks but might not

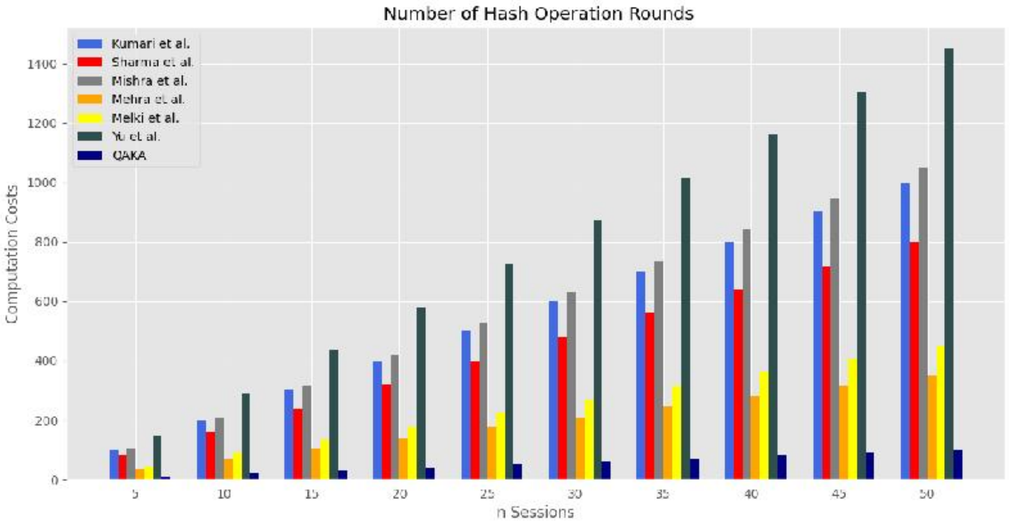


Figure 3.15: The number of Hash operations between User, GWN and SN during the login and authentication phase.

resist Quantum attacks. In order to remain viable in the Quantum era, it is essential to develop new cryptographic primitives that can withstand Quantum threats.

- **Quantum principles:**
  To achieve security, Quantum-based solutions rely on Quantum principles such as No-cloning, classical computing has no substitute for these principles.

- **Key Distribution:**
  Existing authentication schemes rely on classical key distribution methods, such as public keys; they do not incorporate QKD, which utilizes the principles of quantum mechanics to provide secure key distribution.

- **Integration:**
  Integrating quantum-based solutions into existing schemes is not simple as substantial modifications and investments are required. As per our analysis, adapting classical authentication techniques[91] to Quantum-based solutions is not feasible.

3.4.2 Performance Evaluation

The performance of the QAKA protocol is analyzed with other recently proposed work characterized by the number of hash-operation rounds, the number of messages exchanged and the number of time stamps. The results of performance comparisons are depicted in Figures 3.15, 3.16 and 3.17. According to the analysis, the number of hash operations computed and messages exchanged for the secure user login and authentication phase is much less than that of other IoT authentication schemes. Table 3.2 represents the comparative analysis of the above-listed items regarding the role played by the User, Gateway Node and Sensor Node.

Table 3.2: Comparative analysis of QAKA protocol with other IoT authentication protocols

Computation costs	**Year**	**Authors**	**User**	**Gateway Node**	**Sensor Node**
The number of Hash Operation Rounds	2016	Kumari et al.[146]	7	7	6
	2018	Sharma et al.[147]	10	6	None
	2018	Mishra et al.[120]	7	6	8
	2019	Mehra et al.[102]	3	2	2
	2020	Melki et al.[90]	5	4	None
	2021	Yu et al.[22]	11	9	7
	Proposed	QAKA	1	1	0
The number of messages exchanged	2016	Kumari et al.[146]	4	4	3
	2018	Sharma et al.[147]	6	3	None
	2018	Mishra et al.[120]	5	11	3
	2019	Mehra et al.[102]	6	9	3
	2020	Melki et al.[90]	5	3	None
	2021	Yu et al.[22]	4	6	3
	Proposed	QAKA	2	4	2
The number of time stamps exchanged	2016	Kumari et al.[146]	1	1	1
	2018	Sharma et al.[147]	1	1	None
	2018	Mishra et al.[120]	1	2	1
	2019	Mehra et al.[102]	1	1	2
	2020	Melki et al.[90]	2	1	None
	2021	Yu et al.[22]	1	2	1
	Proposed	QAKA	0	0	0

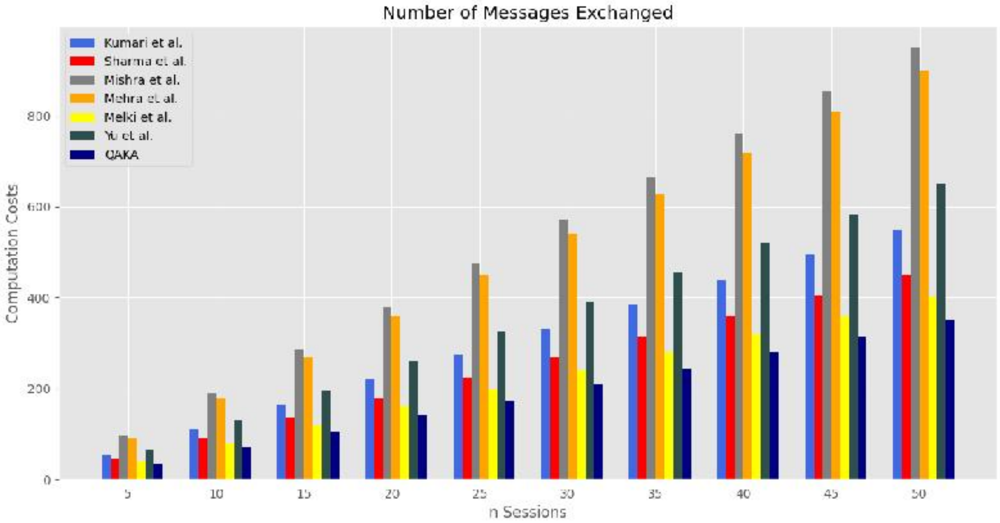


Figure 3.16: The number of messages exchanged between the User, GWN and SN during the login and authentication phase.

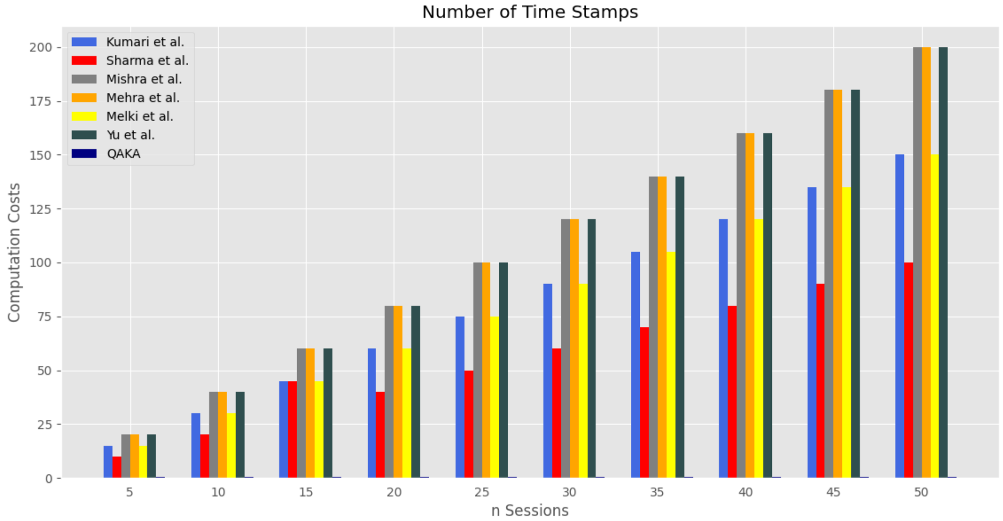


Figure 3.17: The number of time stamps exchanged between User, GWN and SN.

3.4.3 Discussions on Attacks

The analysis of security characteristics in the proposed scheme as compared to other authentication schemes are presented in Table 3.3 The security threats addressed by the QAKA protocol are briefly explained as:

- **Gateway node bypassing attack**: This attack is considered a scenario in which an attacker directly accesses data shared by sensor nodes without participating in the gateway node. Such an attack is impossible in our scheme as both QSN and the user register on GWN by sharing user details as $A_i'{=}f(ID_{USER}\|Puk)$. It is the responsibility of GWN to run an authentication step to authenticate both the user and QSN. The GWN verifies the user information by verifying the following: $\{\{|\phi^{(i)}\rangle_{U1}, |\phi^{(i)}\rangle_{U2}\}_{i=1:m}, Puk, Prk, sk, |\psi^{(i)}_{UIN}\rangle\}$.

- **Gateway impersonation attack**: It could also be some untrusted GWN pretending to be the message recipient without forwarding them. Additionally, the entities are correlated with each other by generating a maximally entangled state as: $|\phi^{(i)}\rangle_{GHZ} = \frac{1}{\sqrt{2}}(|0^{(i)}\rangle_{U1}|0^{(i)}\rangle_{U2}|0^{(i)}\rangle_{GW}|0^{(i)}\rangle_{SN} + |1^{(i)}\rangle_{U1}|1^{(i)}\rangle_{U2}|1^{(i)}\rangle_{GW}|1^{(i)}\rangle_{SN})$. The legitimate GWN can retrieve the user information by measuring $|\phi^{(i)}\rangle_{GW}$.The correlation between GWN, QSN and Users using GHZ states makes this attack impossible.

- **Gateway node capture attack**: This is considered a malicious gateway controlled by an attacker. In this scenario, our protocol generates an authenticated key using the BB84 protocol before establishing any communication. The user information $|\phi^{(i)}_{U2}\rangle$ is retrieved by only legitimate GWN by applying H-Basis $\{|+\rangle, |-\rangle\}$. Therefore, an adversary may not run the login and authentication step by performing a node capture attack.

- **Privileged insider attack**: A person internal to an organization with the right to access the system would not take advantage of our system. In our protocol, the

Table 3.3: QAKA Protocol Security Comparison

Security Consider-ation	[148]	[117]	[149]	[102]	[150]	[151]	[152]	Proposed (QAKA)
Gateway node bypassing	–	✓	–	✓	✓	–	✓	✓
Gateway IA	–	✓	✓	✓	✓	–	✓	✓
Gateway node capture	✓	✓	–	–	✓	–	✓	✓
Privileged insider attack	✓	✓	–	–	✓	–	✓	✓
Traffic–analysis	–	–	–	–	–	✓	–	✓
Eavesdropping identification	–	✓	✓	–	✓	✓	✓	✓
Key-exchange problem	–	–	–	–	✓	✓	✓	✓
Man-in-the-middle	–	–	–	✓	✓	–	✓	✓
Mutual Authentication	✓	✓	✓	✓	✓	✓	✓	✓
Forward Secrecy	–	–	–	✓	✓	–	–	✓
Sensor IA	–	✓	–	✓	✓	–	–	✓
Future Quantum Attacks	–	–	–	–	✓	✓	–	✓
Entanglement	–	–	–	–	✓	–	✓	✓
User Anonymity	–	–	✓	✓	–	–	✓	✓
User IA	–	–	✓	✓	✓	–	✓	✓
Smart Card attack	–	✓	✓	–	–	–	–	✓
Offline PW	–	✓	–	✓	–	–	–	✓
Offline ID Guessing attack	–	–	–	✓	–	–	–	✓
Replay Attack	–	–	✓	✓	–	–	–	✓
Unauthorized Login	–	–	✓	✓	✓	✓	✓	✓
Suitable for IoT	–	–	✓	–	✓	✓	–	✓
Suitable for WSN	✓	✓	✓	✓	✓	✓	✓	✓
Denial-of-Service	–	–	–	✓	–	–	✓	✓
AVISPA	–	–	–	✓	–	–	–	✓

information is not stored as a sequence of plain text; rather, it is in the superposition of qubits as:$|\phi^{(i)}_{U1}\rangle$, $|\phi^{(i)}_{U2}\rangle$, $|ID_{USER}\rangle$,$|\phi_{QP}\rangle$.Each measurement disturbs the quantum system. Therefore, eavesdropping could easily be identified.

- **Traffic-analysis**: Assuming an attacker listens to network communication to determine application behaviour patterns and the location of critical nodes. Due to Quantum laws, copying or determining the system's state is impossible. Additionally, a new quantum state is created in each step; therefore, an adversary can't determine the system's state.

- **Eavesdropping identification attack**: Any intruder who pretends to be a legitimate user needs to produce GHZ states by encoding process:$|\phi^{(i)}\rangle = |\psi_{USER}\rangle \otimes |\phi\rangle_{GHZ}$.In QAKA, copying any quantum state is impossible due to No-cloning.

- **Key exchange problem**: QAKA utilizes photons' ultimate security for establishing a shared key, sk. The shared key, sk, in our protocol, is generated using BB84 protocol, which requires each entity to generate a key and share only measurement basis on a secure quantum channel. Any eavesdropping in key generation and distribution can easily be identified based on the probability of the outcome received.

- **Man-in-the-middle attack**: In this, an attacker, as an unauthorized entity, interrupts the existing conversation. In our protocol, the quantum states are secured by applying QOWF as $B_i = f(ID_{USER}||Prk)$, which makes it impossible for the adversary to retrieve the exact parameters.

- **Mutual authentication**: Authentication between entities must provide safe communication. As in our work, the GWN and user are authenticated by verifying the $|\phi_{QP}\rangle$. The user login and authentication process run by computing a shared key, sk. The GWN also authenticates the sensor node by verifying swap states as $\{|\psi_{SN1}\rangle, |\psi'_{SN1}\rangle\}$

- **Forward secrecy**: In our protocol, the key generation process exchanges randomly, not qubits. Even if the adversary actively inferred, he may not get the secret key with high probability from the Quantum channel.

- **Sensor IA**: It is possible when the adversary acquires secret sensor information and impersonates him on the server. Our protocol resists this attack, as GWN shares the encoded information received from the user as $|\phi^{(i)}\rangle_{U2}$ with entangled authenticated QSN. The legitimate sensor node can perform operations $\{|+\rangle = I, |-\rangle = Z\}$ using quantum gates, which makes it impossible for an adversary to perform this attack.

- **Futuristic quantum attacks**: Internet communications use classical cryptography schemes, and e-commerce could soon succumb to a quantum attack. In our protocol, the quantum states are computed as $|\psi_{SN2}\rangle, |\psi_{SN1}\rangle and |\psi_{US}\rangle$.Communication takes place by using quantum operations rather than mathematical computation. QAKA effectively realize quantum states and utilizes quantum gates, making our protocol Quantum-resistance.

- **User Anonymity**: Our protocol processes users' secret information using QOWF, making our protocol resistant to user anonymity attacks. QAKA ensure that the user sends his identification details securely to GWN by computing: $|\psi_{USER}\rangle = f(ID_{USER}\|Puk)$.Even if the adversary can retrieve ID_{USER}, the entire state of the user is secured using QOWF, which makes it impossible for an intruder to get into the network.

- **User IA**: Our protocol is resistant to this attack, as impersonation is successful when an adversary can effectively obtain a user's secret information. In our scheme, the state of the user is maximally entangled with legitimate GWN and sensor node: $|\phi^{(i)}\rangle_{GHZ} = \frac{1}{\sqrt{2}}(|0^{(i)}\rangle_{U1}|0^{(i)}\rangle_{U2}|0^{(i)}\rangle_{GW}|0^{(i)}\rangle_{SN} + |1^{(i)}\rangle_{U1}|1^{(i)}\rangle_{U2}|1^{(i)}\rangle_{GW}|1^{(i)}\rangle_{SN})$ Each user has two particles that a legitimate user could only measure in this state. Therefore, performing such an attack is impossible for an adversary.

- **Stolen Smart Card attack**: For future communication, the QGC is issued to users who have successfully registered to the Gateway Node. As QGC operates on qubits $|0\rangle$ and $|1\rangle$, it limits the information an intruder can extract from the system. It contains secret user information as $\{\{|\phi^{(i)}\rangle_{U1}, |\phi^{(i)}\rangle_{U2}\}_{i=1:m}, Puk, Prk, sk, |\psi_{UIN}^{(i)}\rangle\}$ .The user's secret information is secured by generating a Quantum state and applying QOWF. Even if adversaries access user information, QOWF cannot be unmasked.

- **Offline PW**: In this scenario, anyone can get the password stored by the user or administrator. However, unlike the classical authentication model in our scheme, there is no password generation process by the user over an insecure channel. However, in our scheme, a quantum password is provided to the legitimate user with the validity of 10 minutes by a legitimate GWN after successful registration as $\{|\phi_{QP}\rangle\}$.

- **Offline Identity Guessing Attack**: Our scheme also protects against this attack. Anyone can access the user ID but may not evaluate the exact identity due to the superposition of quantum states $|ID_{USER}\rangle$. Therefore, this protocol thwarts an identity-guessing attack.

- **Replay Attack**: The adversary intercepts user credentials and shares them with the server using the authenticated channel. However, the user information due to Quantum No cloning cannot be copied. The secret user information in our protocol is also encoded as $|\phi^{(i)}\rangle = |\psi_{USER}\rangle \otimes |\phi\rangle_{GHZ}$ and represented using Bell-states. The legitimate user can apply the measurement and generate the outcome as $\{00, 01, 10, 11\}_{c1,c0}$. Such information, once computed, changes the outcome of other entangled states. Thus, an adversary can't perform a replay attack.

- **Unauthorized login**: Such an attack is impossible in our protocol as QGC is issued to the legitimate user, which contains user information in the superposition of state as: $\{\{|\phi^{(i)}\rangle_{U1}, |\phi^{(i)}\rangle_{U2}\}_{i=1:m}, Puk, Prk, sk, |\psi_{UIN}^{(i)}\}$.Additionally, we use Quantum Password $\{\phi_{QP}\}$ in our protocol, provided to the user after successfully verifying the user, sk. If anyone tries to log in with the wrong identity and password, the request is immediately forwarded to the GWN, and he may restrict any such request.

- **Denial-of-Service**: There are various versions of this attack, such as jamming, flooding, tampering, misdirection etc. In our protocol, each legitimate user can log into the network using QGC. The QGC is issued to each user by GWN on successful registration. The identity of each user $|\psi_{USER}\rangle = f(ID_{USER}\|Puk)$ is also secured using the encoded state as: $|\phi^{(i)}\rangle = |\psi_{USER}\rangle \otimes |\phi\rangle_{GHZ}$ which could only be retrieved by legitimate GWN. Therefore, it is impossible for the fake user to get into the network and overwhelm GWN.

3.5 Summary

In this chapter, we discussed a novel Quantum Authentication and Key Agreement (QAKA) protocol for secure IoT communication. Our work identified many security shortcomings in the IoT-based mutual authentication protocols that relied on classical cryptography. The novelty of our protocol is that we had considered the uniqueness of GHZ states with the secure key distribution, which can identify eavesdroppers' presence on the IoT communication channel. The proposed scheme is safe from classical attacks such as insider, impersonation and futuristic quantum attacks. Quantum C-Swap gates are utilized for evaluating the similarity between states. The formal verification security analysis using the BAN logic analysis and ROM is provided, which proves QAKA capabilities to defend against various attacks. It is utilized to demonstrate the fulfilment of essential security requirements. We conducted simulations using the AVISPA tool, confirming that QAKA is resilient against security threats like replay and MITM attacks, thereby guaranteeing the safety of our protocol. Our protocol has played a substantial role in paving the way for quantum-based communication in the IoT, facilitating device authentication and the establishment of a secure communication environment within the network.

Chapter 4

QUANTUM-BASED SECURE CRYPTOSYSTEM FOR IoT

4.1 Introduction

Recently, with the advancement in wireless communication, IoT technology can connect and interact with different devices[153]. Due to anytime and anywhere connectivity, IoT devices are now enormously used in healthcare to facilitate real-time services to patients and doctors. Many real-time healthcare applications require continuous monitoring, such as ECG, blood pressure, respiration rate, blood glucose level, etc. [154]. Any deviation in monitoring patient health conditions could be fatal. The security of huge IoT data traffic is a major issue and concern. The classical primitives such as RSA, Exclusively-OR (XOR) functions, AES, One-way hash Function (OWHF), and ECC were widely accepted to provide authentication in IoT-enabled healthcare applications [72].

However, recent advancements in Quantum Computing-based well-known algorithms like Shor's factoring[155] and Grover's database[156] search algorithm [157] have already proven that they could easily solve the classical algorithms such as RSA by exploiting the exponential speedup of Quantum Computers[158].

Therefore, we proposed a Novel Quantum-based Secure Cryptosystem using Mutual Authentication for Healthcare (QSMAH) in IoT by considering the limitations of classical cryptographic schemes. The potential advantage of Quantum Cryptography inspires our scheme. Figure 4.1 represents the proposed QSMAH architecture. It depicts the secret communication among the GWN, CMS, and MP using the process of GHZ states, Teleportation and QKD.

Our unique contribution involves the generation of three particles of GHZ state on IBM Quantum Experience (IQE), using which secret information is shared between legitimate entities. With the specific aim of improving the key distribution process in this paper, we proposed the modified QKD scheme, which involves three communicating entities to participate in the secret Quantum key generation process. In this chapter, we first discuss the proposed Quantum Cryptography-based secure key distribution and mutual authentication protocol. We then present the formal and informal analysis of the proposed protocol. Finally, we present the simulation of the proposed model using the AVISPA tool. In Table4.1, we compared the proposed QSMAH protocol with existing healthcare-based schemes on classical and Quantum Cryptography.

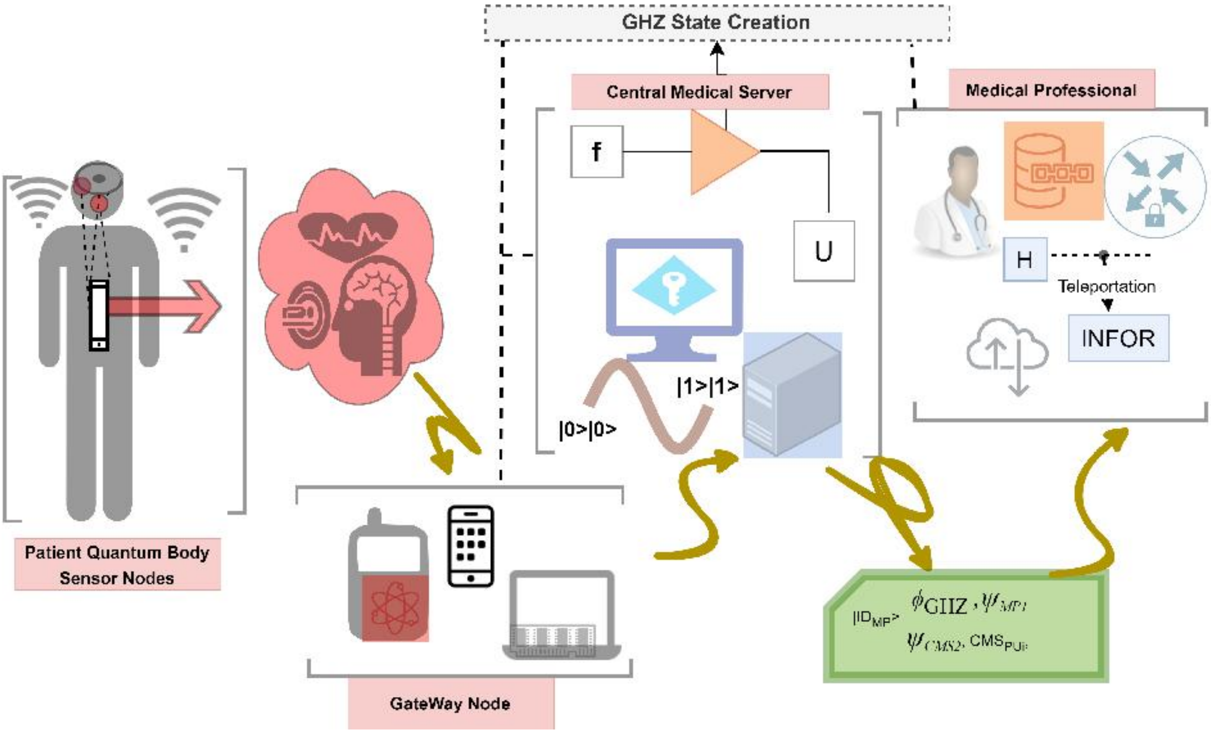


Figure 4.1: Quantum based Healthcare architecture.

Table 4.1: Other researchers work on IoT and Quantum authentication schemes

Research Papers	**Year**	**Objective**	**Tool and Algorithm**	**1**	**2**	**3**	**4**	**5**
Shukla et al.[154]	2021	Identification and authentication of data transmission.	iFog-Simulator	✓	✓	-	-	Model
Elhoseny et al.[159]	2018	Diagnostic test data security in Medical imaging.	AES and RSA	✓	✓	-	-	Model
Xu et al.[160]	2022	Generate Quantum Key	Quantum Computing	✓	-	✓	✓	Model
Mehra et al.[102]	2019	Authentication between the user, SN, and GWN.	AVISPA	✓	-	-	✓	Model
Bahache et al.[161]	2022	Privacy and security of IoT-enabled medical applications	-	✓	✓	-	✓	Survey
Rasool et al.[162]	2021	Provide Quantum advantage in healthcare	-	-	✓	✓	-	Survey
Alsaeed et al.[163]	2022	Identified the requirement of authentication in Internet-based medical things	-	✓	✓	-	✓	Survey
Amin et al.[164]	2018	Ensure MA for transferring Medical data using WSN	AVISPA	✓	✓	-	✓	Model

Research Papers	Year	Objective	Tool and Algorithm	1	2	3	4	5
Sharma et al.[165]	2018	Quantum Cryptography-based Quantum Key agreement for cloud authentication	AVISPA	✓	-	✓	✓	Model
Behra et al.[150]	2017	Usage of GHZ states for mutual authentication	BB84	✓	-	✓	✓	Model
Sk et al.[143]	2020	Effective realization of Quantum teleportation	IQE	✓	-	✓	✓	Model
Li et al.[166]	2017	MA schemes for IoT	RSA and ECC	✓	-	-	✓	Survey
Melki et al.[90]	2020	IoT entities MA and shared session key agreement	X-OR and Hash function	✓	-	-	✓	Model
Proposed Work		MA and KA utilize QC to secure healthcare data.	Quantum Computing, AVISPA	✓	✓	✓	✓	Model

1: Mutual Authentication; 2: Healthcare; 3: Usage of Quantum; 4: Security Considerations; 5: Model/Survey

4.2 Proposed Quantum-Based Secure Cryptosystem using Mutual Authentication for Healthcare (QS-MAH)

This section will detail QSMAH, which provides security and confidentiality features for healthcare in IoT applications. This work proposes Quantum GHZ states for multiuser communication and QKD for secure KA. QSMAH protocol ensures a) Forgery-resistant b) Non-repudiation c) Confidentiality. First, the information associated with each entity, such as Patient, CMS, and MP, cannot be copied. Second, the authorized patient cannot deny the message's legitimacy or data transfer due to undeniable proof produced for authentication and integrity. Finally, all information authorised entities provide remains safe and secure from eavesdropping. The QSMAH protocol comprises five algorithms: as π = (Prep, GENE, REG, login, Auth.). These phases are described as follows:

4.2.1 Preparation Phase

In the preparation phase, the medical administrator provides a secure unique $|ID_{QSN}>$ to each sensor device implanted in the patient's body. As in our scheme, several patients seek advice from several doctors depending on the requirements of the individual. Therefore, each patient and Medical Professional (Doctor or Lab staff) in our scheme is assigned a unique registration ID as $|ID_P>$ and $|ID_{MP}>$ provided by the secure CMS. The Patient's Mobile device as GWN is registered at the secure Clinician Medical Server (CMS) as $|ID_{GW}>$. All entities in our protocol, such as Patient (P$_I$), CMS, and MP, should generate the public and private keys $(P_i(P_{puk}, P_{prk})), (CMS_i(CMS_{puk}, CMS_{prk}), (MP_i(MP_{puk}, MP_{prk}))$.

4.2.2 Generation Phase

In our protocol, by utilizing GHZ states, each entity correlates with the other for secure medical data transfer. The GHZ state between GWN, CMS, and MP is generated to accomplish this goal. Medical sensors monitor the patient's body. The information is transferred from the sensor node to the Gateway device through the secure Quantum channel. Therefore, GHZ states are effectively realized between GWN, CMS, and MP for secure data transmission. The structural representation of GHZ states, along with probabilities on IQE, are represented in Figure 4.2. The GHZ states for three particles can generally be expressed as Eq.4.1 and 4.2:

$$|\Psi^{+}{}_{0,0\oplus r,0\oplus u} >_{ABC}= \frac{1}{\sqrt{2}}(|0, 0 \oplus r, 0 \oplus u > +|1, 1 \oplus r, 1 \oplus u >) and \tag{4.1}$$

$$|\Psi^{+}{}_{0,0\oplus r,0\oplus u} >_{ABC}= \frac{1}{\sqrt{2}}(-1)^{0\oplus u}(|0, 0 \oplus r, 0 \oplus u > -|1, 1 \oplus r, 1 \oplus u >) \tag{4.2}$$

where, r,u $\varepsilon 0, 1$. The GHZ state can be generated for QSMAH as in Eq.4.3,4.4 and 4.5:

$$G1 = \frac{1}{\sqrt{2}}(|0 > +|1 >) \otimes |00 >= \frac{1}{\sqrt{2}}(|000 > +|100 >) \tag{4.3}$$

$$G2 = U_{CNOT}^{ctrl=q0}|G1 >= \frac{1}{\sqrt{2}}(|000 > +|110 >) \tag{4.4}$$

$$G3 = U_{CNOT}^{ctrl=q0}|G2 >= \frac{1}{\sqrt{2}}(|000 > +|111 >) \tag{4.5}$$

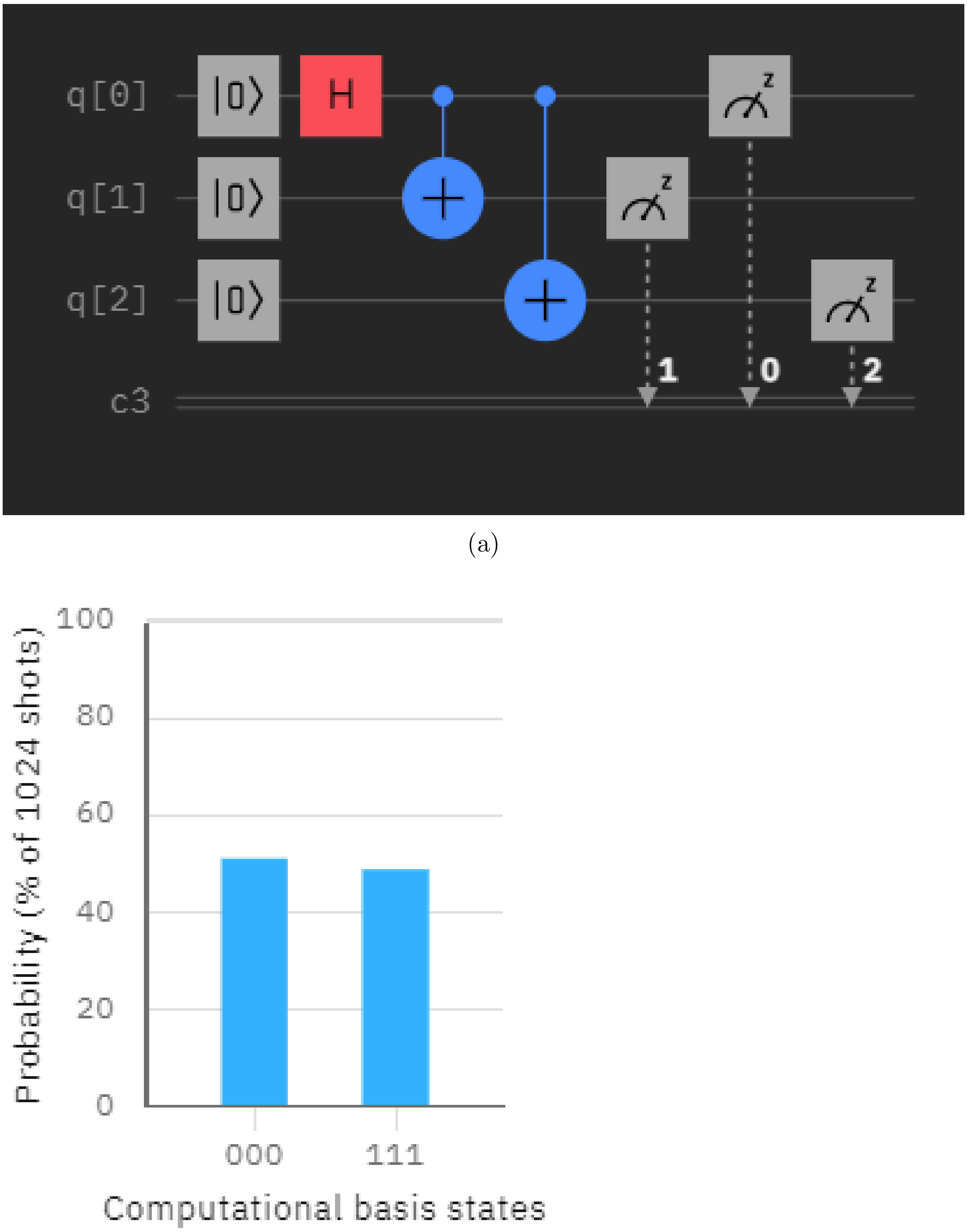
Finally, the output GHZ state is generated as in Eq.4.6:

$$|\varnothing_{GHZ}^{(i)} >= \frac{1}{\sqrt{2}}(|0^{(i)} >_{GWN} |0^{(i)} >_{CMS} |0^{(i)} >_{MP} +|1^{(i)} >_{GWN} |1^{(i)} >_{CMS} |1^{(i)} >_{MP}) \tag{4.6}$$

Where 1 $\leq$ i $\leq$ n represents the distinctive, unique identification number of each communicating entity i $\varepsilon\{0, 1\}^n$.Here, $|\varnothing_{GHZ}^{(i)} >_{i=1:m} = |\varnothing_{GHZ}^{(1)} >, |\varnothing_{GHZ}^{(1)} > ...|\varnothing_{GHZ}^{(m)} >$ represents orthogonal GHZ entangled states. A unique GHZ state is generated by CMS whenever a patient wants to establish secure communication with a medical professional.

4.2.3 Registration Phase

Each patient and MP must register with CMS before sharing secret data in this phase. In this section, we explain the patient registration process through GWN and then move on to CMS. Then, we discuss the MP registration for CMS.



(a)

(b)

Figure 4.2: (a): Quantum three qubits GHZ states on IBM Quantum Experience (IQE); (b): Probabilistic outcome of GHZ state on IBM Quantum Experience (IQE)

4.2.3.1 Patient Registration

In this phase, before each patient registers onto CMS through GWN. The sensors inside the patient's body sense the information and transfer it through Gateway to CMS. There are more chances that an intruder can perform an impersonation attack in the registration phase. Therefore, we utilize Quantum Cryptography for secure communication and data transfer. Generating a Quantum key establishes the secret communication between GWN and CMS. Figure4.3 depicts the registration process's structural representation. It represents the Patient Registration onto CMS through GWN. The detailed steps for the registration of legitimate patients to GWN using the Quantum Channel are described as follows:

Step 1: Each patient is assigned a Unique ID before registration. The patient provides their unique identity and chooses to create a password as ID_P, PW_p for registration onto GWN(Mobile device).

Step 2: The superposition state of patient credentials is computed by Gateway Node (Mobile Device) for verification as $|ID_P>, |PW_p>$.

Step 3: Initially, GWN has the following credentials: $|ID_p>$ and $|PW_p>$.Using which GWN can compute: $Q1 = h(ID_p||PW_p)$.

Step 4: After verifying patient identities, the GWN chooses a Random Code Word(RCW), which is in the superposition of states $|CWGW>$ and measure it in $\{|+>, |->\}$ basis.

Step 5: GWN sends the measurement Basis $\{|+>, |->\}$ to patient BSN.

Step 6: Sensor Node chooses a Random Code Word (RCW), which is in the superposition of states $|CWSN>$.Sensor Node applies the measurement in $\{|+>, |->\}$ basis. The sensor node applies a Pauli matrix (error correction) on its qubits as in Eq4.7:

$$|+> \to Iand|-> \to Z \tag{4.7}$$

Step 7: The GWN verifies the measurement results: $M^U_{SN} = M'^U_{GW}$. The Gateway discards the registration process if the measurement results do not match. Otherwise, GWN successfully registers sensor nodes.

Step 8: The GWN generates a string of maximally entangled states as in Eq.4.8:

$$|\varnothing>_{GHZ} = \frac{1}{\sqrt{2}}(|0^{(i)}>_{GWN} |0^{(i)}>_{CMS} |0^{(i)}>_{MP} + |1^{(i)}>_{GWN} |1^{(i)}>_{CMS} |1^{(i)}>_{MP}) \tag{4.8}$$

Step 9: The GWN computes the information as in Eq.4.9:

$$Q2 = h(ID_p||ID_{SN_i}||ID_{GW}||ID_{MP}) \tag{4.9}$$

Considering the above state as in 4.9, the superposition of state as $|\psi_{Q2}>= \alpha|0> +\beta|1>$. The state mentioned above represents the important Sensor Node information; therefore, the GWN encodes the state $|\psi_{Q2}>$into its entangled qubit as in Eq.4.10 .After encoding the Quantum state is represented in Eq.4.11 and the complete Quantum state is as described in Eq.4.12 as :

$$|\phi>_{GWSN} = Q2 \bigotimes |\varnothing>_{GHZ} \tag{4.10}$$

$$= (\alpha|0> +\beta|1)_{Q2} \bigotimes (|000> + |111>)_{GHZ} \tag{4.11}$$

$$= (\alpha|0>_{Q2} (\frac{|000+|111>}{\sqrt{2}}) + \beta|1)_{Q2}(\frac{|000+|111>}{\sqrt{2}}) \bigotimes (|000>+|111>)_{GHZ} \tag{4.12}$$

The H-Gate on the first qubit $|Q2>$ and CNOT on its part of a qubit, GWN changes the Quantum system state as in Eq.4.13:

$$= \alpha(\frac{|0>+|1>}{\sqrt{2}})_{Q2} \bigotimes (\frac{|000+|111>}{\sqrt{2}})_{GHZ} + \beta(\frac{|0>-|1>}{\sqrt{2}})_{Q2} \bigotimes (\frac{|100+|011>}{\sqrt{2}})_{GHZ} \tag{4.13}$$

The total Quantum state of the system becomes as in Eq.4.14:

$$\begin{aligned} &= \alpha \\ &\frac{|0_{GW}0_{GW}0_{CMS}0_{MP}>+|0_{GW}1_{GW}1_{CMS}1_{MP}>+|1_{GW}0_{GW}0_{CMS}0_{MP}>+|1_{GW}1_{GW}1_{CMS}1_{MP}>}{2} \\ &+ \beta \\ &\frac{|0_{GW}1_{GW}0_{CMS}0_{MP}>+|0_{GW}0_{GW}1_{CMS}1_{MP}>-|1_{GW}1_{GW}0_{CMS}0_{MP}>-|1_{GW}0_{GW}1_{CMS}1_{MP}>}{2} \end{aligned} \tag{4.14}$$

The above equation can be written in bell state as in Eq.4.15:

$$\begin{aligned} &= \frac{1}{2}(|\Phi^{+}>_{GW}(\alpha|0_{CMS}0_{MP}>+\beta|1_{CMS}1_{MP}>)+|\Phi^{-}>_{GW}(\alpha|0_{CMS}0_{MP}>-\beta|1_{CMS}1_{MP}>)+ \\ &|\Psi^{+}>_{GW}(\alpha|1_{CMS}1_{MP}>+\beta|0_{CMS}0_{MP}>)+|\Psi^{-}>_{GW}(\alpha|1_{CMS}1_{MP}>-\beta|0_{CMS}0_{MP}>)) \end{aligned} \tag{4.15}$$

Step 10: After encoding, the GWN measures his part of the qubits $|\Phi^{\pm}>_{GW} and|\Psi^{\pm}>_{GW}$.
Then, according to the bell measurement outcomes as in Eq.4.16:

$$(00, 01, 10, 11)_{c1,c0} \Rightarrow INFO_R \tag{4.16}$$

GWN applies after applying partial measurement of two entangled qubits and sends those qubits as classical bits using the classical channel to CMS. Based on the above information received from the GWN through the teleportation process, the CMS stores the following information as $INFO_R$ to retrieve appropriate state $|Q2>_{GW}$.
Step 11: After receiving the above information from the GWN. The CMS generates the Secret Quantum Key with GWN. CMS and GWN make use of Quantum Random Number Generator (QRNG) to generate random keys as: $\{k^1_{CMS}, k^2_{CMS}, k^3_{CMS}, ..., k^n_{CMS}\}$ and $\{k^1_p, k^2_p, k^3_p, ..., k^n_p\}$, where $k^u_{CMS}, k^u_p \varepsilon$ 0,1,u =1,2,.n , where n is the length of the shared private key.
Step 12: CMS and GWN will calculate the hash value of the corresponding random key and publish results to each other as $h(k_{CMS})$ and $h(k_p)$.
Step 13: Considering the 8n particles GHZ entangled states, CMS divide them into the sequences as in Eq.4.17:

$$S_H = \{S^1_H, S^2_H, S^3_H, ...S^n_H\} \tag{4.17}$$

Where, S^j_H is the jth particle of H=CMS, GWN and j=1,2,3. . . . . . 8n
Step 14: CMS applies the Z-Basis measurement on his particles and obtains the

results as in Eq.4.18:

$$M_{CMS} = \{M_1, M_2, M_3.......M_n\} \tag{4.18}$$

Step 14: Based on the above measurement results, CMS computes the following information as in Eq.4.19:

$$Q_{CMS_k} = M^U_{CMS} \bigotimes k^u_{CMS} \tag{4.19}$$

and send the Q_{CMS_k} to GWN.
Step 15: GWN also measures the particles in Z-Basis and obtains the results as in Eq.4.20:

$$M_{GW} = \{M_1, M_2, M_3......M_n\} \tag{4.20}$$

Based on the above measurement results, GWN computes the following information: $Q_{GW_k} = M^U_{GW} \otimes K^u_p$.GWN send the Q_{GW_k} to CMS.
Step 16: It is apparent that $M^U_{GW} = M^U_{CMS}$. Therefore, according to M^U_{CMS} CMS extracts the $h(k_p)$ from Q_{GW_k} and compute $h(k_p)$ and match: $h(k_p) = h'(k_p)$. In case of any mismatch, then CMS discards the registration process. If both values match, then CMS accepts the final key as in Eq.4.21:

$$Q_{k_H} = k^u_{CMS} \bigoplus K^u_p \tag{4.21}$$

CMS will Acknowledge GWN for successfully generating the secret Quantum key.
Step 17: Once CMS generates the Quantum key then, according to M^U_{GW} GWN extracts the k^u_{CMS} from Q_{CMS_k} and compute $hk_{CMS} = h^{'}(k_{CMS})$. In case of any mismatch, then GWN discards the registration process, else GWN accepts the final key as:$Q_{k_H} = k^u_{CMS} \bigoplus K^u_p$.
Step 18: After the successful generation of the final Quantum key, CMS computes the final registration information as in Eq.4.22:

$$|\psi^{(i)}_{CMS1} >= h(ID_p||ID_{GW}||ID_{CMS}||Q_{k_H}||P_{puk}||CMS_{puk}||ID_{SN_i}) \tag{4.22}$$

Step 19: Based on the above information, GWN registered onto the CMS and computes the final information as in Eq.4.23:

$$|\psi^{(i)}_{GW} >= h(ID_p||ID_{GW}||ID_{CMS}||Q_{k_H}||ID_{SN_i}) \tag{4.23}$$

4.2.3.2 Medical Professional Registration onto GWN

In our protocol, the MP must register before accessing the patient's confidential information stored on the medical server. The MP could also be contacted during emergencies directly through patient IoT devices. Therefore, there is a higher chance that an intruder could provide false advice to patients and leak important medical data by executing an MITM attack. Our protocol ensures that legitimate MP identity must be verified before sharing patient medical details with MP. The steps for registration of MP onto CMS are structurally represented in Figure 4.4and the detailed explanation of which is as follows:
Step 1: Initially, the GHZ state between GWN and CMS is established as in Eq.4.24

$$|0^{(i)} >_{GHZ}= \frac{1}{\sqrt{2}}(|0^{(i)} >_{GWN} |0^{(i)} >_{CMS} |0^{(i)} >_{MP} +|1^{(i)} >_{GWN} |1^{(i)} >_{CMS} |1^{(i)} >_{MP}) \tag{4.24}$$

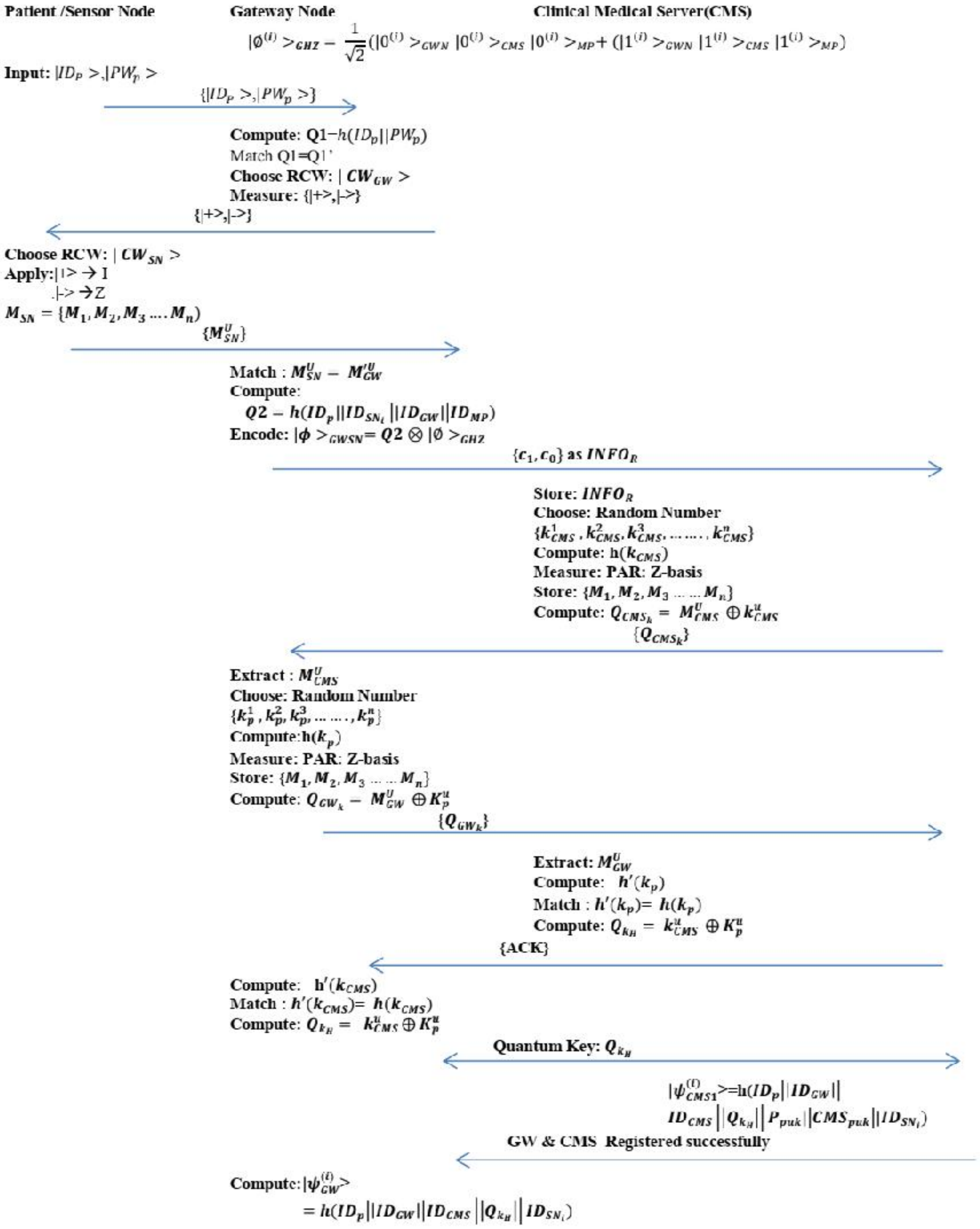

Patient /Sensor Node
Gateway Node
Clinical Medical Server(CMS)
$|\emptyset^{(i)}>_{GHZ} = \frac{1}{\sqrt{2}}(|0^{(i)}>_{GWN}|0^{(i)}>_{CMS}|0^{(i)}>_{MP} + (|1^{(i)}>_{GWN}|1^{(i)}>_{CMS}|1^{(i)}>_{MP})$
Input: $|ID_P>, |PW_p>$
$\{|ID_P>, |PW_p>\}$
Compute: $Q1 = h(ID_p||PW_p)$
Match Q1=Q1'
Choose RCW: $|CW_{GW}>$
Measure: {|+>,|->}
{|+>,|->}
Choose RCW: $|CW_{SN}>$
Apply:|+> → I
|-> → Z
$M_{SN} = \{M_1, M_2, M_3 \dots M_n\}$
$\{M_{SN}^U\}$
Match : $M_{SN}^U = M_{GW}'^U$
Compute:
$Q2 = h(ID_p||ID_{SN_i}||ID_{GW}||ID_{MP})$
Encode: $|\phi>_{GWSN} = Q2 \otimes |\emptyset>_{GHZ}$
$\{c_1, c_0\}$ as $INFO_R$
Store: $INFO_R$
Choose: Random Number
$\{k_{CMS}^1, k_{CMS}^2, k_{CMS}^3, \dots, k_{CMS}^n\}$
Compute: $h(k_{CMS})$
Measure: PAR: Z-basis
Store: $\{M_1, M_2, M_3 \dots M_n\}$
Compute: $Q_{CMS_k} = M_{CMS}^u \oplus k_{CMS}^u$
$\{Q_{CMS_k}\}$
Extract : M_{CMS}^U
Choose: Random Number
$\{k_p^1, k_p^2, k_p^3, \dots, k_p^n\}$
Compute:$h(k_p)$
Measure: PAR: Z-basis
Store: $\{M_1, M_2, M_3 \dots M_n\}$
Compute: $Q_{GW_k} = M_{GW}^U \oplus K_p^u$
$\{Q_{GW_k}\}$
Extract: M_{GW}^U
Compute: $h'(k_p)$
Match : $h'(k_p) = h(k_p)$
Compute: $Q_{k_H} = k_{CMS}^u \oplus K_p^u$
{ACK}
Compute: $h'(k_{CMS})$
Match : $h'(k_{CMS}) = h(k_{CMS})$
Compute: $Q_{k_H} = k_{CMS}^u \oplus K_p^u$
Quantum Key: Q_{k_H}
$|\psi_{CMS1}^{(i)}> = h(ID_p||ID_{GW}||ID_{CMS}||Q_{k_H}||P_{puk}||CMS_{puk}||ID_{SN_i})$
GW & CMS Registered successfully
Compute: $|\psi_{GW}^{(i)}> = h(ID_p||ID_{GW}||ID_{CMS}||Q_{k_H}||ID_{SN_i})$

Figure 4.3: Patient Registration.

Step 2: MP input credentials onto CMS as: $\{|ID_{MP}>, |PW_{MP}>\}$. Each legitimate MP can submit the registration details based on GHZ states.
Step 3: CMS will match the$|ID_{MP}>$ from the registered medical professional list and store the final information as in Eq.4.25:

$$Q3 = (ID_p||PW_p) \tag{4.25}$$

In case of any mismatch between credentials submitted by MP, then CMS will discard the registration process.
Step 4: CMS will be able to receive the $\{c_1, c_0\}$ as $INFO_R$ from GWN based on GHZ states.
Step 5: CMS gives $\{|ID_{CMS}>, |CMS_{puk}>\}$ to MP.MP will be able to receive the $\{c_1, c_0\}$ as $INFO_R$ from GWN based on GHZ states. It computes: $\{|ID_{MP}>, |MP_{puk}>\}$ and send it to CMS.
Step 6: After receiving the $\{|ID_{MP}>, |MP_{puk}>\}$ from MP CMS will compute the Quantum Secret Key with MP. To generate the Quantum Secret key, the following steps need to be performed between CMS and MP:
CMS and MP make use of a Quantum Random Number Generator (QRNG) to generate random keys as in Eq.4.26

$$\{k^1_{CMS}, k^2_{CMS}, k^3_{CMS}, ..., k^n_{CMS}\}and\{k^1_{MP}, k^2_{MP}, k^3_{MP}, ..., k^n_{MP}\} \tag{4.26}$$

Where, k^u_{CMS}, k^u_{MP} ϵ 0,1, u =1,2,. . . .,n. Considering the 8n particles GHZ entangled states, CMS divide them into the sequences in Eq.4.27:

$$S_H = \{S^1_H, S^2_H, S^3_H, ...S^n_H\} \tag{4.27}$$

Where, S^j_H is the jth particle of S_H, H = {CMS,MP} and j= {1, 2,3. . . . . . 8n}. CMS applied the Z-Basis measurement on his particles and obtained the results as in Eq.4.28

$$M_{MP} = \{M_1, M_2, M_3......M_n\} \tag{4.28}$$

and send the Q_{CMS_K} to MP. MP also measured the particles in Z-Basis and obtained the results as in Eq.4.29:

$$M_{MP} = \{M_1, M_2, M_3, ...M_n\} \tag{4.29}$$

Based on the above measurement results, MP computes the following information: $Q_{MP_K} = M^U_{MP} \bigoplus k^U_{MP}$ and sends the Q_{MP_K} to CMS. Based on the above measurement results, CMS computes the following information as in Eq.4.30:

$$Q_{CMS_K} = M^U_{CMS} \bigoplus k^u_{CMS} \tag{4.30}$$

It is apparent that $M^U_{MP} = M^U_{CMS}$. Therefore, according to M^U_{CMS} CMS extracts the h(k_{MP}) from Q_{MP_K} and compute h(k_{MP}) and match: h(k_{MP}) = h'(k_{MP}). In case of any mismatch then, CMS discards the registration process. If both values match, then CMS accepts the final key as in Eq. 4.31

$$Q_{K_H} = k^u_{MP} \bigoplus K^u_{CMS} \tag{4.31}$$

CMS will acknowledge GWN to generate the secret Quantum key successfully. once CMS generates the Quantum key, then according to M^U_{MP} MP extracts the k^{u}_{CMS} from Q_{CMS_K} and computes h(k_{CMS}) = h'(k_{CMS}). In case of any mismatch, then MP discards the registration process else, MP accepts the final key as in Eq.4.32:

$$Q_{K_H} = k^{u}_{CMS} \bigoplus K^{u}_{MP} \tag{4.32}$$

Step 7: After the successful generation of Quantum Key, MP will compute as in Eq.4.33:

$$|\Psi^{(i)}_{MP1} >= h(ID_{MP}||Q_{k_H}||ID_{CMS}||MP_{puk}||CMS_{puk}||INFO_R) \tag{4.33}$$

and send it to CMS for final registration.

Step 8: CMS will accept the registration process by accepting the information from MP as ID_{MP} and $|\Psi^{(i)}_{MP1} >$. Based on the information received from MP, CMS will compute the following as in Eq.4.34 and 4.35:

$$|\Psi^{(i)}_{CMS2} >= h(ID_{MP}||Q_{k_H}||ID_{CMS}||MP_{puk}||CMS_{puk})and \tag{4.34}$$

$$QGHC : (|\Psi^{(i)}_{CMS2} >, |\Psi^{(i)}_{MP1} >, |\phi^{(i)}_{GHZ} >, CMS_{puk}) \tag{4.35}$$

Based on the above information, MP is registered with CMS. After successful registration, a QGHC containing MP information for secure login is generated for each legitimate MP. QGHC is equipped with Quantum memory to be used for future secure communication.

4.2.4 Login and Authentication Phase

Initially, the GHZ state is generated between the legitimate entities as in Eq.4.36:

$$|0^{(i)} >_{GHZ}= \frac{1}{\sqrt{2}}(|0^{(i)} >_{GWN} |0^{(i)} >_{CMS} |0^{(i)} >_{MP} +|1^{(i)} >_{GWN} |1^{(i)} >_{CMS} |0^{(i)} >_{MP}) \tag{4.36}$$

The overall workflow is depicted in Figure4.5.

The structural representation of the login and authentication phase is represented in Figure4.7. The detailed explanation of the login and authentication phase is described as follows:

Step 1: The registered Patient submits his identity to GWN as: $|ID_p >, |PW_p >$.

Step 2: The GWN verifies the user identities by computing Q4$'$ = h(ID_p||PW$_p$)and match if $Q1 \not\equiv Q4'$.If it does not match the GWN, discard the patient's login. If it matches, GWN allows the patient to successfully login into the system.

Step 3: After receiving patient requests for login, the GWN, CMS, and MP will generate Quantum Key for secure communication. The secret Quantum Key generation will take place as follows:

(a) GWN, CMS, and MP will generate Quantum Random Numbers as in Eq.4.37:

$$\{k^{1}_{CMS}, k^{2}_{CMS}, k^{3}_{CMS}, ..., k^{n}_{CMS}\}and\{k^{1}_{MP}, k^{2}_{MP}, k^{3}_{MP}, ..., k^{n}_{MP}\}, \tag{4.37}$$

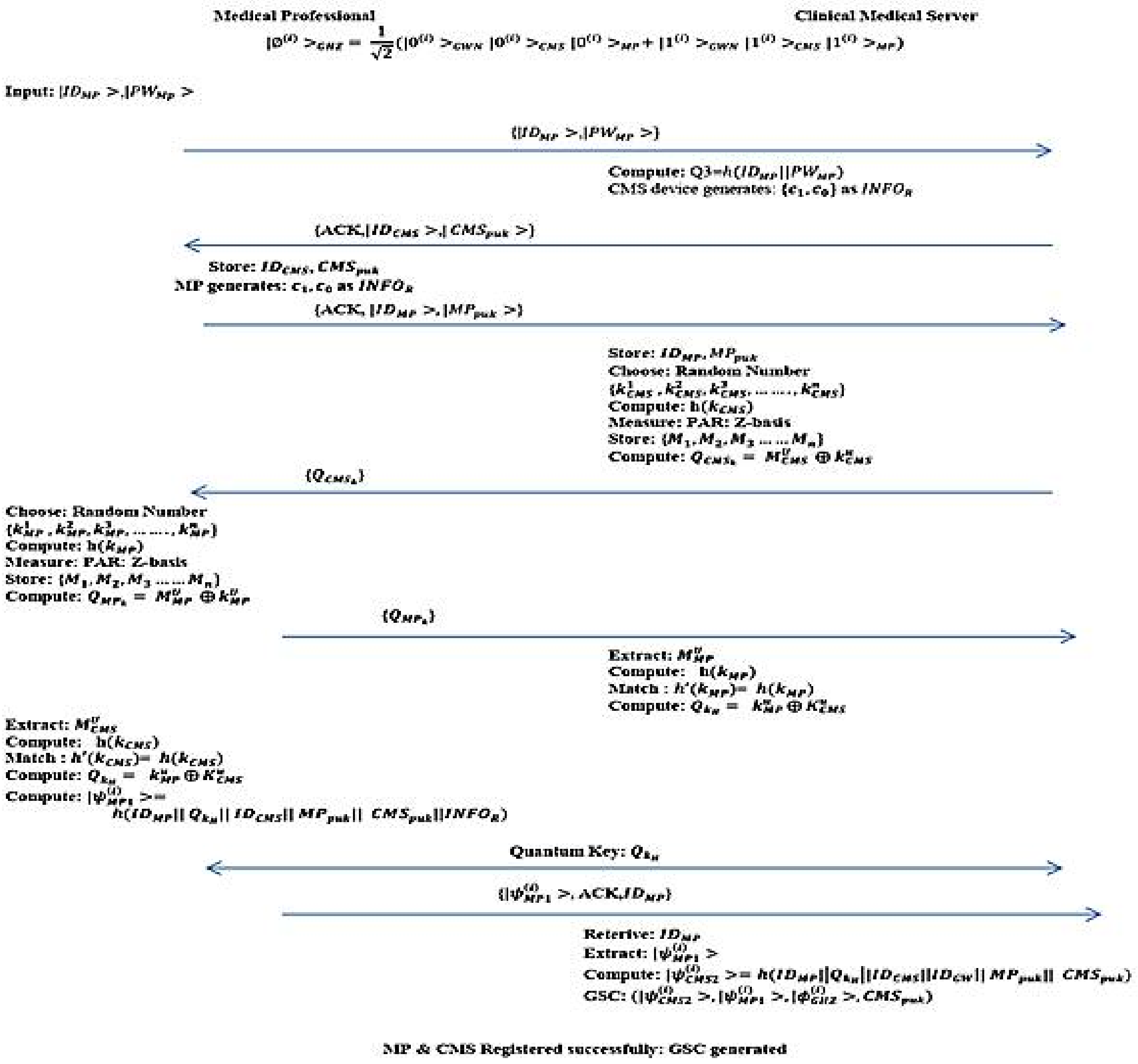

Medical Professional
Clinical Medical Server
$|\varnothing^{(i)}>_{GHZ} = \frac{1}{\sqrt{2}}(|0^{(i)}>_{GWN}|0^{(i)}>_{CMS}|0^{(i)}>_{MP} + |1^{(i)}>_{GWN}|1^{(i)}>_{CMS}|1^{(i)}>_{MP})$
Input: $|ID_{MP}>, |PW_{Mp}>$
$(|ID_{MP}>, |PW_{MP}>)$
Compute: Q3=$h(ID_{MP}||PW_{MP})$
CMS device generates: $\{c_1, c_6\}$ as $INFO_R$
$\{ACK, |ID_{CMS}>, |CMS_{puk}>\}$
Store: ID_{CMS}, CMS_{puk}
MP generates: c_1, c_6 as $INFO_R$
$\{ACK, |ID_{MP}>, |MP_{puk}>\}$
Store: ID_{MP}, MP_{puk}
Choose: Random Number
$\{k^1_{CMS}, k^2_{CMS}, k^3_{CMS}, \ldots\ldots, k^n_{CMS}\}$
Compute: h(k_{CMS})
Measure: PAR: Z-basis
Store: $\{M_1, M_2, M_3 \ldots\ldots M_n\}$
Compute: $Q_{CMS_k} = M^U_{CMS} \oplus k^u_{CMS}$
$\{Q_{CMS_k}\}$
Choose: Random Number
$\{k^1_{MP}, k^2_{MP}, k^3_{MP}, \ldots\ldots, k^n_{MP}\}$
Compute: h(k_{MP})
Measure: PAR: Z-basis
Store: $\{M_1, M_2, M_3 \ldots\ldots M_n\}$
Compute: $Q_{MP_k} = M^U_{MP} \oplus k^u_{MP}$
$\{Q_{MP_k}\}$
Extract: M^U_{MP}
Compute: h(k_{MP})
Match : $h'(k_{MP}) = h(k_{MP})$
Compute: $Q_{k_H} = k^u_{MP} \oplus K^u_{CMS}$
Extract: M^U_{CMS}
Compute: h(k_{CMS})
Match : $h'(k_{CMS}) = h(k_{CMS})$
Compute: $Q_{k_H} = k^u_{MP} \oplus K^u_{CMS}$
Compute: $|\psi^{(i)}_{MP1}> = h(ID_{MP}||Q_{k_H}||ID_{CMS}||MP_{puk}||CMS_{puk}||INFO_R)$
Quantum Key: Q_{k_H}
$\{|\psi^{(i)}_{MP1}>, ACK, ID_{MP}\}$
Reterive: ID_{MP}
Extract: $|\psi^{(i)}_{MP1}>$
Compute: $|\psi^{(i)}_{CMS2}> = h(ID_{MP}||Q_{k_H}||ID_{CMS}||ID_{GW}||MP_{puk}||CMS_{puk})$
GSC: $(|\psi^{(i)}_{CMS2}>, |\psi^{(i)}_{MP1}>, |\phi^{(i)}_{GH2}>, CMS_{puk})$
MP & CMS Registered successfully: GSC generated

Figure 4.4: Medical Professional Registration

Where,k^u_{CMS},k^u_{MP} ϵ $\{0,1\}$,u =1, 2, . . . , n and n is the length of the shared private key. GWN, CMS, and MP will calculate the hash value of the corresponding random key and publish results to each other as: $h(k_{CMS})$,$h(k_{MP})$,$h(k_p)$.

(b) CMS, GWN, and MP by applying Z-Basis measurement on his particles and obtain the results: $M_{CMS} = M^1_{CMS}, M^2_{CMS}, M^3_{CMS}$........, M^n_{CMS}denote the bits of M_{CMS}. Similarly, $M_{GW} = M^1_{GW}, M^2_{GW}, M^3_{GW}$........, M^n_{GW} denote the bits of M_{GW}, while $M_{MP} = M^1_{GW}, M^2_{GW}, M^3_{MP}$........, M^n_{MP} denote the bits of M_{MP} corresponding to the KA.
In case of no eavesdropping, the measurement results obtained should be equivalent to each other as in Eq.4.38:

$$M_{CMS} = M_{GW} = M_{MP} \tag{4.38}$$

CMS calculates: $Q_{CMS_K} = M^U_{CMS} \oplus k^u_{CMS}$ and send Q_{CMS_K} to GWN and MP. Similarly, GWN computes: $Q_{GW_K} = M^U_{GW} \oplus k^u_p$ and send Q_{GW_K} to CMS and MP; finally, MP calculates $Q_{MP_K} = M^U_{MP} \oplus k^u_{MP}$ and send Q_{MP_K} to CMS and GWN.

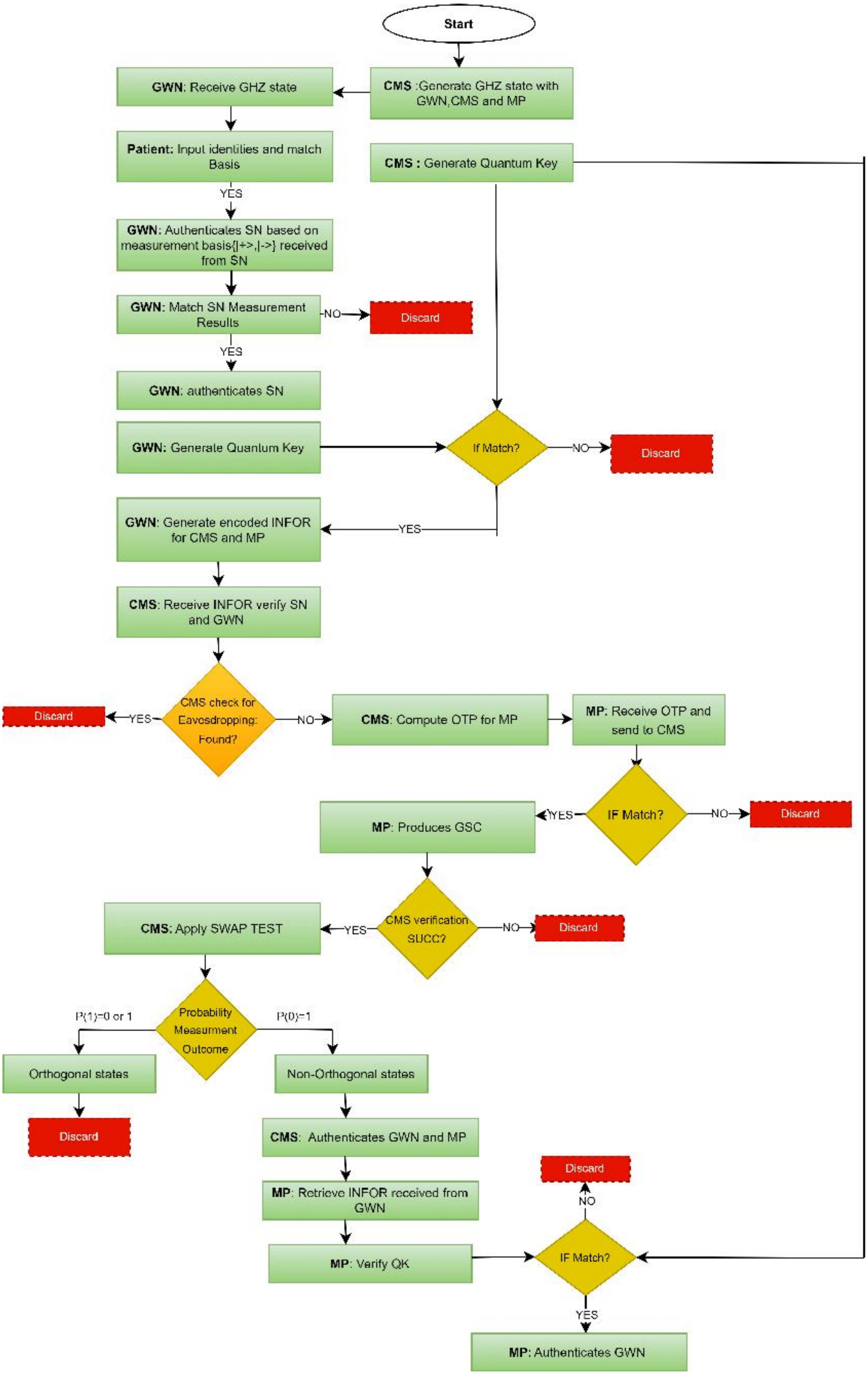

Start
CMS :Generate GHZ state with GWN,CMS and MP
GWN: Receive GHZ state
Patient: Input identities and match Basis
CMS : Generate Quantum Key
YES
GWN: Authenticates SN based on measurement basis{|+>,|->} received from SN
GWN: Match SN Measurement Results
NO
Discard
YES
GWN: authenticates SN
GWN: Generate Quantum Key
If Match?
NO
Discard
YES
GWN: Generate encoded INFOR for CMS and MP
CMS: Receive INFOR verify SN and GWN
Discard
YES
CMS check for Eavesdropping: Found?
NO
CMS: Compute OTP for MP
MP: Receive OTP and send to CMS
MP: Produces GSC
YES
IF Match?
NO
Discard
CMS: Apply SWAP TEST
YES
CMS verification SUCC?
NO
Discard
P(1)=0 or 1
Probability Measurment Outcome
P(0)=1
Orthogonal states
Non-Orthogonal states
Discard
CMS: Authenticates GWN and MP
MP: Retrieve INFOR received from GWN
Discard
NO
MP: Verify QK
IF Match?
YES
MP: Authenticates GWN

Figure 4.5: Flowchart of Login and authentication phase

CMS according to M_{CMS} extract the k_p^u and k_{MP}^U from Q_{GW_K} and Q_{MP_K}.The CMS calculates and verifies the hash value of
h(k_{MP}) = h'(k_{MP}) and h(k_p) = h'(k_p).If the values match, then CMS will accept the final key as in Eq.4.39:

$$QK : k_{MP} \oplus k_p \oplus k_{CMS} \tag{4.39}$$

MP according to M_{MP} extract the k_p^u and k_{CMS}^u from Q_{GW_K} and Q_{CMS_K}.If the values match, then MP will accept the final key as in Eq.4.40:

$$QK : k_{MP} \oplus k_p \oplus k_{CMS} \tag{4.40}$$

GWN according to M_{GW} extract the k_p^u and k_{GW}^u from Q_{CMS_K} and Q_{MP_K}. It calculates and verifies the hash value of h(k_p) = h'(k_p) and h(k_{MP}) = h'(k_{MP}). If the values match, then GWN will accept the final key as QK: $k_{MP} \oplus k_p \bigoplus k_{CMS}$. The Quantum secret key is generated and verified by legitimate entities individually. It helps in preventing Forward secrecy attacks.

Step 4: After successfully generating a Quantum secret key by legitimate authorized entities. GWN verifies the appropriate BSN by generating $|CW_{GW} >$ in superposition and measuring it in $\{|+>, |->\}$ basis. GWN instead of sending the code word $|CW_{GW} >$ to patient BSN share measurement basis $\{|+>, |->\}$ with SN.
Step 5: Once the SN receives the measurement basis $\{|+>, |->\}$.SN chooses appropriate codeword $|CW_{GW} >$ and performs error correction by applying the Pauli matrix as in Eq.4.41:

$$|+> \rightarrow Iand|-> \rightarrow Z \tag{4.41}$$

Step 6: Based on the measurement basis SN authenticates the legitimate GWN for future secure communication.
After correcting errors, the SN sends the measurement results to GWN.GWN verify the M_{SN} received from SN by matching with their results as in Eq.4.42:

$$M_{SN}^U = M_{GW}^{\prime U} \tag{4.42}$$

If it matches, then based on the measurement results, GWN retrieves the appropriate SN identity ID_{SN} and computes $h'(P_{puk})$. GWN matches h'(P_{puk}) = $h(P_{puk})$. If the Public key (PUK) matches, SN successfully proves his identity to GWN and allows data sharing with GWN. Based on the retrieved and verified information, GWN and SN calculate the session key as in Eq.4.43:

$$SK_{GW-SN} = h(M_R||ID_{GW}||ID_{SNi}) \tag{4.43}$$

Therefore, GWN authenticates legitimate SN for sharing data. It prevents any sensor node impersonation and GWN bypassing attack.

Step 7: Once GWN verifies the legitimate SN, then GWN secures SN information along with registered MP ID_{MP}, Patient identity ID_p and ID_{GW} as in Eq.4.44:

$$Q2 = h(ID_p||ID_{SN_i}||ID_{GW}||ID_{MP}) \tag{4.44}$$

Considering the above state as in Eq.4.44, the superposition of state as $|\psi_{Q2}>= \alpha|0> +\beta|1>$. The state mentioned above represents the important patient medical data; therefore, the GWN encodes the state as in Eq.4.45:

$$|\phi>_{GWSN}= Q2 \otimes |\varnothing>_{GHZ} \tag{4.45}$$

Afterwards, the user carries out entanglement measurement on his first two qubits. The four qubits bell state can be written in Eq. 4.46

$$\begin{aligned}|\phi>_{GWSN}= \frac{1}{2}\{|\Phi^+>_{GW} (\alpha|0_{CMS}0_{MP}> +\beta|1_{CMS}1_{MP}>) + |\Phi^->_{GW} (\alpha|0_{CMS}0_{MP}> \\ -\beta|1_{CMS}1_{MP}>) + |\Psi^+>_{GW} (\alpha|1_{CMS}1_{MP}> \\ +\beta|0_{CMS}0_{MP}>) + |\Psi^->_{GW} (\alpha|1_{CMS}1_{MP}> +\beta|0_{CMS}0_{MP}>)\}\end{aligned} \tag{4.46}$$

After encoding, the GWN measures his part of the qubits $|\Phi^\pm>_{GW}$ and $|\Psi^\pm>_{GW}$.

Then, according to the bell measurement outcomes as $(00,01,10,11)_{c1,c0} \Rightarrow INFO_R$. GWN applies after applying partial measurement of two entangled qubits and sends those qubits as classical bits using the classical channel to CMS and MP for future secure communication. It prevents any traffic analysis attack. Additionally, GWN also sends Q5 = $h(INFO_R||SK_{GW-SN})$

securely to CMS. On successful login of GWN, the CMS checks the authenticity of GWN by retrieving $INFO_R$.

Step 8: Once classical information { $\{c1, c0\}$ as $INFO_R\}$ received from GWN to CMS as in Eq.4.47:

$$\{c1, c0\} \rightarrow 00, 01, 10, 11 \tag{4.47}$$

CMS, after receiving information from the GWN, first verify the time taken by the message. It deletes the message received by GWN if $TS_{CMS} - TS1 > \triangle T$. Else, retrieve Q5 as $h(INFO_R||SK_{GW-SN})$ store $INFO_R$. Then it extracts classical bits received from GWN c_1, c_0 and apply Pauli (Error Correction) Matrix on his part of Qubits as stated in Table 4.2 and corrects the state of his Qubit to recover the original state as in Eq.4.48

$$Q2 = h(ID_p||ID_{SN_i}||ID_{GW}||ID_{MP}) \tag{4.48}$$

Table 4.2: QuantumPauli gate operation on qubit measurement

GWN Measurement	**00**	**01**	**10**	**11**
Value of CMS qubit	$\alpha\|0> +\beta\|1>$	$\alpha\|1> +\beta\|0>$	$\alpha\|0> \beta\|1>$	$\alpha\|1> \beta\|0>$
Quantum Gate	Identity(I)	X==NOT	Phase flip (Z)	NOT and Z gate

Step 9: Once CMS receives the appropriate information; it will store $Q2 = h(ID_p||ID_{SN_i}||ID_{GW}||ID_{MP})$.

Then, CMS will generate a serial number as S for each legitimate patient with a legitimate BSN to be verified by a registered Medical professional. CMS will send that information to the appropriate GWN as in Eq.4.49:

$$Q6 = h(S||TS2||ID_{GW}) \tag{4.49}$$

Step 10: GWN, after receiving information from the CMS, first verify the time taken by Q6. The GWN deletes the received message if $TS_{GW} - TS2 > \triangle T$. Else, retrieve Q6. Once GWN receives the Serial number (S) from CMS, it can log in successfully into the system.
Step 11: The CMS will generate OTP for legitimate MP.
Step 12: After receiving information from the CMS, MP first verifies the time taken by the OTP. The received OTP is invalid if $TS_{MP} - TS3 > \triangle T$. Otherwise, MP input $|ID_{MP} >, |PW_{MP} >$ and produces GSC as GSC $\leftarrow |\psi^{(i)}_{CMS2} >, |\psi^{(i)}_{MP1} >, CMS_{pui}, |\phi^{(i)}_{GHZ} >$ and send the information mentioned above along with OTP to GWN.

Step 13: Based on the above information, CMS verifies the time taken by the message. It will not consider the message if $TS_{CMS} - TS4 > \triangle T$. Otherwise, verify OTP and allow MP to successfully log into the system. CMS also computes based on information received from MP as in Eq.4.50

$$|\psi'^{(i)}_{CMS2} >= h(ID_{MP}||Q_{K_H}||ID_{CMS}||ID_{GW}||MP_{puk}||CMS_{puk}) \tag{4.50}$$

GWN then applies the SWAP Test on $|\psi^{(i)}_{MP1} >, |\psi'^{(i)}_{MP1} >$ for verifying legitimate MP. The SWAP-Gate [150] is illustrated in Figure4.6. It represents if two states are identical if $|q_0 >$ will be in state $|0 >$. However, if$|q_0 >$ will be $|0 >$ or$|1 >$ with equal probability, then two states are orthogonal. Both states are equal or not depending upon the probability measurement outcome as in Eq.4.51:

$$P(1) = \frac{1}{2}(1| < \phi|\Psi > |^2) and P(0) = \frac{1}{2}(1 + | < \phi|\Psi > |^2) \tag{4.51}$$

Where P (1) represents the probability of measuring 1 on qubit $|q_0 >$ and P(0) represents the probability of measuring $|0 >$ on the first qubit. Two states are identical if $P(1) = 0$ and $P(0) = 1$. However, if $P(0) < 1$, then states are not identical.

After successfully evaluating swap states, the CMS authenticates the MP and allows him to log in to the system. But if states do not match, the ancilla qubits are in both $|0 >$ and $|1 >$ states. The CMS analyzes the probability associated with each outcome as $|\Psi^{(i)}_{MP1} > |\Psi^{(i)}_{MP1} > \geqslant K_1, K_1$ is constantly decided by CMS. At the end of step 13, the CMS and the MP possess a session key for further data transfer as in Eq.4.52:

$$SK_{CMS-MP} = h(S||ID_p||ID_{MP}||ID_{CMS}) \tag{4.52}$$

Step 14: CMS also verifies $|\Psi'^{(i)}_{CMS1} >$ By using a one-way function, if the information matches, then CMS computes Eq.4.53:

$$Q7 = h(S||ID_p||ID_{GW}||ID_{MP}) \tag{4.53}$$

Step 15: Based on the above information, GWN verifies the time taken by the message. If $TS_{GW} - TS5 > \triangle T$, then it deletes the received message else, GWN also computes Eq.4.54:

$$|\Psi_{GW-SN} >= h(S||ID_p||ID_{GW}||ID_{MP}||ID_{CMS}) \tag{4.54}$$

On successful completion of steps 14 and 15, the CMS and the GWN mutually authenticated and possess a session key for further data transfer as in Eq.4.55:

$$SK_{GW-CMS} = h(S||ID_{GW}||ID_{CMS}||SK_{CMS-MP}) \tag{4.55}$$

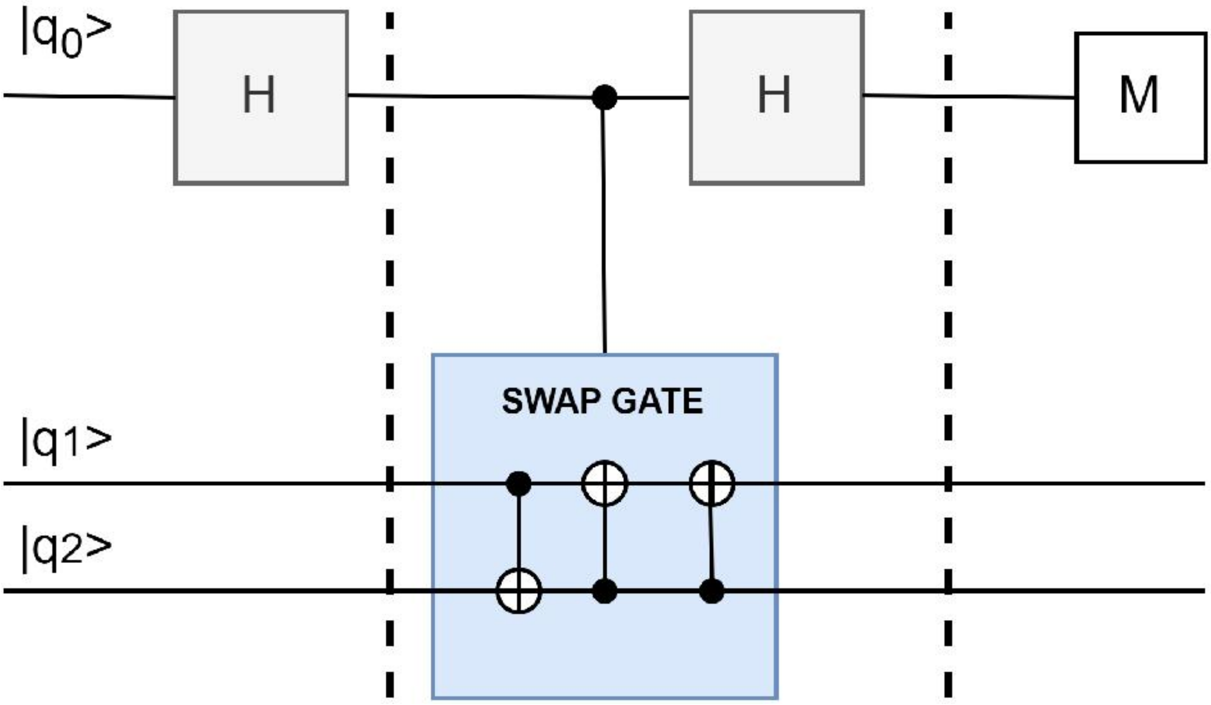


Figure 4.6: QuantumSWAP-Gate

Step 16: MP, after generating the session key with CMS as (SK_{CMS-MP}) verify the time taken by the message. If $TS_{MP} - TS6 > \triangle T$, then it deletes the received message else, based on $INFO_R$, as represented in 4.3. It will identify encoded information as in Eq.4.56:

$$Q2 = h(ID_p||ID_{SN_i}||ID_{GW}||ID_{MP}) \tag{4.56}$$

Table 4.3: Quantum Pauli gate operation on qubit measurement

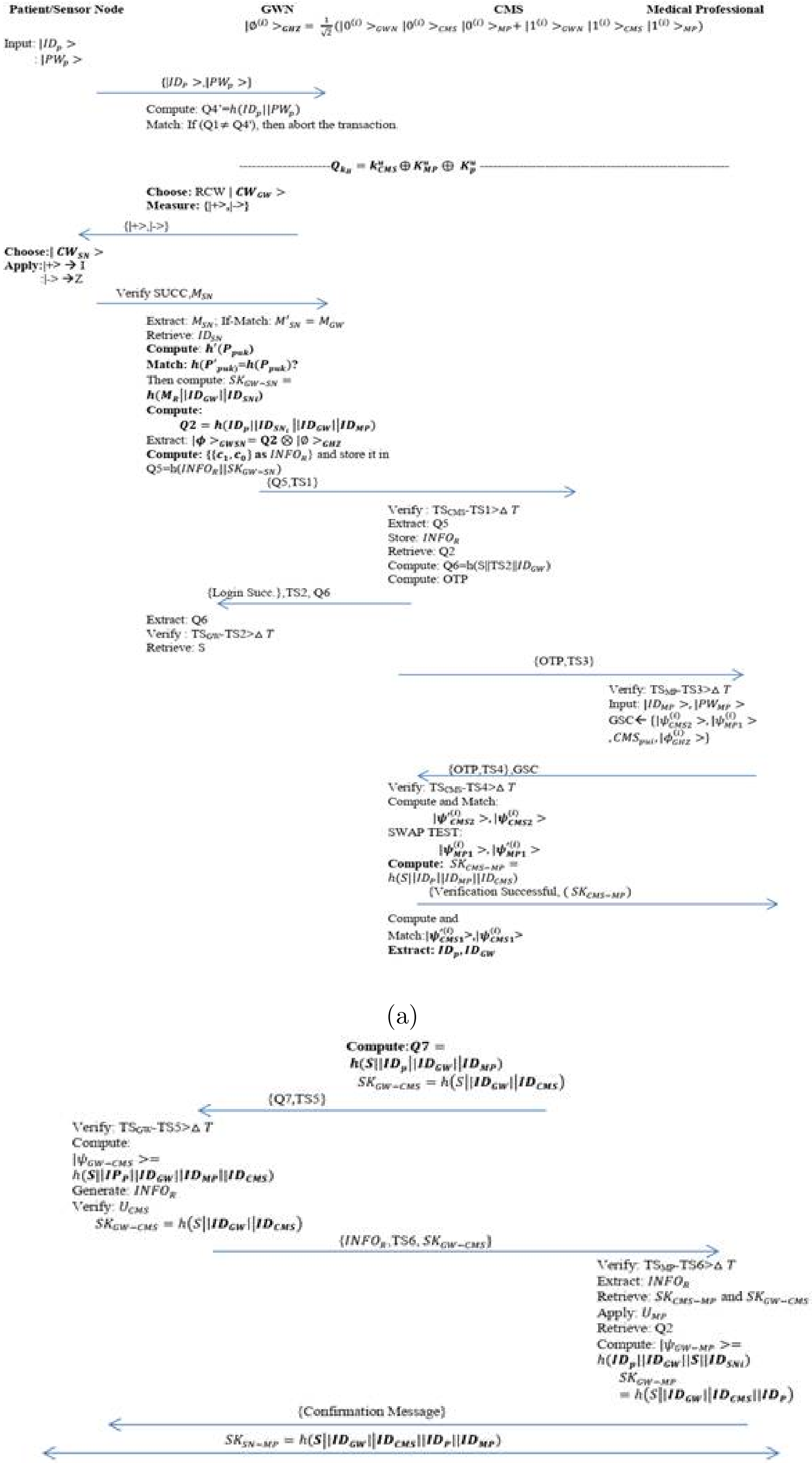
GWN Measurement	**00**	**01**	**10**	**11**
Quantum Gate	Identity(I)	X==NOT	Phase flip (Z)	NOT and Z gate

Based on the above information, MP authenticates the appropriate GWN and allows him to contact MP in an emergency.MP will also compute the appropriate information as: $|\Psi_{GW-MP} >= h(ID_p||ID_{GW}||S||ID_{SN_i})$ based on the information received from legitimate GWN. This process will prevent impersonation attacks.
At the end of this step, GWN and MP will compute the following information for future communication as in Eq.4.57:

$$SK_{GW-MP} = h(S||ID_{GW}||ID_{CMS}||ID_P) \tag{4.57}$$

Step 17: On successful completion of step 16, MP will send a ”Final Message” to legitimate GWN with the following information as in Eq.4.58:

$$SK_{SN-MP} = h(S||ID_{GW}||ID_{CMS}||ID_P||ID_{MP}) \tag{4.58}$$



(a)

(b)

Figure 4.7: Login and Authentication

4.3 Security Analysis

In this section, we present the formal security analysis of the proposed schemes using the BAN logic to prove the goal of our protocol. We also discuss the informal analysis of our proposed scheme.

4.3.1 Formal Proof using BAN Logic

The BAN analysis is to prove that the Patient, GWN, CMS, and MP in our protocol will agree on the Session Key. The basic notations are defined below in table 4.4 for defining rules, making assumptions, and providing proof in BAN logic. M and N are statements, and U and V are principals.

Table 4.4: Symbols and Abbreviations in BAN Logic Analysis

Notation	**Meaning**
U $\mid\equiv$ M	U believes M
U $\triangleleft$ M	U receives/Sees M
U $\mid\sim$ M	U sometimes stated M
U $\mid\Rightarrow$ M	U has complete authority over M
$\sharp$(M)	M is fresh
$U \overset{K}{\leftrightarrow}$ V	U and V share information using shared key K
(M)$_{QK}$	M is hashed under the key Quantum Key
(M,N)	The formulas are combined and then hashed.
$\{M\}_{k_{bs}}$	M is encrypted with key k
QK	Quantum key
k$_{as}$	Public Key
k$_{bs}$	Private Key
SK	Session Key
C'	The measure Quantum bit String
U$_{-}>$ V:?	U sends V ? through Quantum Channel
C$_1$(x), C$_2$(x),C$_3$(x)	Entangled String shared with GWN, CMS, and MP.
Bs_{GW} , Bs_{SN}	Sensor and Gateway Basis

BAN logic rules in our proofs are as follows:

R1: Message –Meaning rule: $\frac{U|\equiv V \ U\overset{k_{bs}}{\longleftrightarrow}V, U\triangleleft\{M\}_{k_{bs}}}{U|\equiv V|\sim M}$

R2: Nonce verification rule: $\frac{U|\equiv V\#(M), U|\equiv V|\sim M}{U|\equiv V|\equiv M}$

R3: Jurisdiction rule:$\frac{U|\equiv V|\Rightarrow M, U|\equiv V|\equiv(M)_{QK}}{U|\equiv M}$

R4: Freshness Rule: $\frac{U|\equiv\#(M)}{U|\equiv\#(M,N)}$

R5: Quantum key rule: $\frac{U|\equiv\#(M), U|\equiv V|\equiv M}{U|\equiv U\overset{QK}{\longleftrightarrow}V}$

R6: Session key rule:$\frac{U|\equiv\#(M),U|\equiv V|\equiv M}{U|\equiv U\overset{QK}{\longleftrightarrow}V}$

R7: Believe rule: $\frac{U|\equiv(M,N)}{U|\equiv M}$

The QSMAH protocol is considered secure and valid; based on BAN logic, the following goals as:

Goal 1: $GWN| \equiv (GWN \overset{sk}{\leftrightarrow} SN)$
Goal 2: $GWN| \equiv (GWN \overset{sk}{\leftrightarrow} CMS)$
Goal 3: $CMS| \equiv (CMS \overset{sk}{\leftrightarrow} GWN)$
Goal 4: $CMS| \equiv GWN| \equiv (CMS \overset{sk}{\leftrightarrow} GWN)$
Goal 5: $MP| \equiv (MP \overset{sk}{\leftrightarrow} CMS)$
Goal 6: $MP| \equiv CMS| \equiv (MP \overset{sk}{\leftrightarrow} CMS)$
Goal 7: $CMS| \equiv MP| \equiv (CMS \overset{sk}{\leftrightarrow} MP)$
Goal 8: $CMS| \equiv MP| \equiv (GWN \overset{sk}{\leftrightarrow} MP)$
Goal 9: $MP| \equiv SN| \equiv (MP \overset{sk}{\leftrightarrow} GWN)$

The idealized form of QSMAH is analyzed considering the messages exchanged using BAN logic as stated below:

- **M1:** $SN \to GWN : (|CW_{GW} >, SN \overset{sk}{\leftrightarrow} GWN)_{M_R}$
- **M2:** $GWN \to CMS : (TS1, GWN \overset{SK}{\longleftrightarrow} CMS)_{Q5}$
- **M3:** $CMS \to MP : (TS3, CMS \overset{SK}{\longleftrightarrow} MP)$
- **M4:** $GWN \to MP : (TS6, (GWN \overset{SK}{\longleftrightarrow} MP)_{INFO_R}$

We listed some of the assumptions from A1 to A35, which are considered to prove the goals are written as follows:

A1: $GWN| \equiv SN| \equiv (GWN \overset{M_R}{\longleftrightarrow} SN)_{Bs_G}$

A2: $SN| \equiv GWN| \equiv (GWN \overset{M_R}{\longleftrightarrow} SN)_{Bs_G}$

A3: $GWN| \equiv \sharp(|CW_{GW} >)$

A4: $SN| \equiv \sharp(|CW_{GW} >)$

A5: $SN| \equiv GWN| \Rightarrow (GWN \xleftrightarrow{SK_{GW-SN}} SN)$

A6: $GWN| \equiv (GWN \overset{Q5}{\longleftrightarrow} CMS)$

A7: $CMS| \equiv GWN| \equiv (GWN \overset{Q5}{\longleftrightarrow} CMS)$

A8: $CMS| \equiv (GWN \overset{Q6}{\longleftrightarrow} CMS)$

A9: $GWN| \equiv CMS| \equiv (GWN \overset{Q6}{\longleftrightarrow} CMS)$

A10: $MP| \equiv \sharp(TS3)$

A11: $CMS| \equiv \sharp(TS4)$

A12: $CMS| \equiv \sharp(OTP)$

A13: $GWN| \equiv \sharp(OTP)$

A14: $CMS| \equiv (GWN \overset{QK}{\longleftrightarrow} MP)$

A15: $MP| \equiv (GWN \overset{QK}{\longleftrightarrow} CMS)$

A16: $GWN| \equiv CMS| \equiv (CMS \overset{Q5}{\longleftrightarrow} MP)$

A17: $CMS| \equiv (GWN \overset{MP}{\longleftrightarrow}_{GSC} MP)$

A18: $MP| \equiv GWN| \Rightarrow (CMS \overset{SK_{CMS-MP}}{\longleftrightarrow} MP)$

A19: $GWN| \equiv \sharp(TS5)$

A20: $GWN| \equiv CMS| \equiv (GWN \overset{Q6}{\longleftrightarrow} CMS)$

A21: $CMS| \equiv GWN| \equiv (GWN \overset{Q7}{\longleftrightarrow} CMS)$

A22: $GWN| \equiv CMS| \Rightarrow (CMS \overset{Q7}{\longleftrightarrow} GWN)$

A23: $GWN| \equiv CMS| \Rightarrow (CMS \overset{SK_{GW-CMS}}{\longleftrightarrow} GWN)$

A24: $MP| \equiv \sharp(TS6)$

A25: $CMS| \equiv GWN| \Rightarrow (CMS \overset{INFO_R}{\longleftrightarrow} MP)$

A26: $MP| \equiv GWM| \Rightarrow (CMS \overset{INFO_R}{\longleftrightarrow} MP)$

A27: $CMS| \equiv GWN| \Rightarrow (CMS \overset{INFO_R}{\longleftrightarrow} GWN)$

A28: $MP| \equiv GWN| \Rightarrow (SN \overset{SK_{SN-MP}}{\longleftrightarrow} MP)$

A29: $SN| \equiv GWN| \equiv (GWN \overset{SK}{\longleftrightarrow} CMS)_{Q4}$

A30: $GWN| \equiv (GWN \overset{QK}{\longleftrightarrow} CMS)$

A31: $CMS| \equiv (CMS \overset{QK}{\longleftrightarrow} MP)$

A32: $SN| \equiv GWN| \equiv (GWN \overset{SK}{\longleftrightarrow} CMS)_{|\phi > GWSN}$

A33: $SN| \equiv GWN| \equiv (GWN \overset{ID_p}{\longleftrightarrow} CMS)_{Q4}$

A34: $CMS| \equiv (GWN \overset{QK}{\longleftrightarrow} CMS)$

A35: $CMS| \equiv (GWN \overset{OTP}{\longleftrightarrow} CMS)$

Now, the sequences of main proof to achieve the goal stated above are provided below:
According to message 1 and seeing the rule, we get:

P1:$GWN \lhd (|CW_{GW} >, SN \overset{sk}{\leftrightarrow} GWN)_{M_R}$

P2 is obtained on the basis of P1, R6 and A33 as:

P2:$SN| \equiv GWN| \equiv (GWN \overset{ID_p}{\longleftrightarrow} CMS)_{Q4}$

P3 is obtained on the basis of P2, R1 and A2 as:

P3:$SN| \equiv GWN| \sim (Bs_G, GWN \overset{M_R}{\longleftrightarrow} SN)$

P4 is obtained on the basis of P3, R2 and A1 as:

P4:$GWN| \equiv SN| \equiv (\sharp|CW_{SN} >, GWN \overset{M_R}{\longleftrightarrow} SN)_{Bs_{GW}}$

P5 is obtained on the basis of P4, R4 and A2 as:

P5:$SN| \equiv GWN| \equiv (\sharp|CW_{GW} >, GWN \overset{M_R}{\longleftrightarrow} SN)_{Bs_{GW}}$

P6 is obtained on the basis of P5,R6 and A5 as:

P6: $GWN| \equiv (GWN \overset{SK}{\longleftrightarrow} SN)$ **[Goal 1]**

According to message 2 and seeing the rule, we get

P7: $CMS \triangleleft (TS1, GWN \overset{SK}{\longleftrightarrow} CMS)_{Q5}$

P8 is obtained on the basis of P7, A30 and R5 as:

P8: $GWN| \equiv CMS| \equiv (GWN \overset{QK}{\longleftrightarrow} CMS)$

P9 is obtained on the basis of P8, A34, and R6 as:

P9: $CMS| \equiv GWN| \equiv (GWN \overset{QK}{\longleftrightarrow} CMS)$

P10 is obtained on the basis of P9, R1 and A32 as:

P10: $SN| \equiv GWN| \equiv (GWN \overset{SK}{\longleftrightarrow} CMS)_{|\phi>_{GWSN}}$

P11 is obtained on the basis of P10, A29 and R7 as:

P11: $CMS| \equiv (CMS \overset{sk}{\leftrightarrow} GWN)$ **[Goal 3]**

P12 is obtained on the basis of P11, A27and R3 as:

P12: $CMS| \equiv GWN| \Rightarrow (CMS \overset{INFO_R}{\longleftrightarrow} GWN)_{|\phi>_{GWSN}=Q2\otimes|\emptyset>GHZ}$

P13 is obtained on the basis of P12, A7 and R7 as:

P13:$CMS| \equiv GWN| \equiv (TS1, GWN \overset{Q5}{\longleftrightarrow} CMS)$

P14 is obtained on the basis of P13, A23 and R6 as:

P14: $GWN| \equiv CMS| \Rightarrow (CMS \overset{SK_{GW-CMS}}{\longleftrightarrow} GWN)$

P15 is obtained on the basis of P14, A23 and R7 as:

P15: $GWN| \equiv (GWN \overset{sk}{\leftrightarrow} CMS)$ **[Goal 2]**

P16 is obtained on the basis of P15, A9 and R3 as:

P16: $GWN| \equiv CMS| \Rightarrow (TS2, GWN \overset{Q6}{\longleftrightarrow} CMS)$

P17 is obtained on the basis of P16, A35, and R1:

P17: $GWN| \equiv CMS| \sim (TS3, GWN \overset{OTP}{\longleftrightarrow} CMS)$

According to message 3 and seeing the rule, we get

P18: $MP \triangleleft (TS3, CMS \overset{SK}{\longleftrightarrow} MP)$

P19 is obtained on the basis of P18, A31 and R5 as

P19: $CMS| \equiv (CMS \overset{QK}{\longleftrightarrow} MP)$

P20 is obtained On the basis of P19, A17 and R1 as:

P20: $CMS| \equiv (TS1, CMS \overset{MP_{GSC}}{\longleftrightarrow} MP)$

P21 is obtained On the basis of P20, A18 and R7 as:

P21: $MP| \equiv (MP \overset{sk}{\leftrightarrow} CMS)$ **[Goal 5]**

P22 is obtained on the basis of P21, A18 and R2 as:

P22: $CMS| \equiv (TS4, CMS \overset{MP_{GSC}}{\longleftrightarrow} MP)$

P23 is obtained On the basis of P22, A11 and R6, as:

P23: $MP| \equiv CMS| \equiv (MP \overset{sk}{\leftrightarrow} CMS)$ **[Goal 7]**

P24 is obtained on the basis of P23, A18 and R3 as:

P24:$MP| \equiv CMS| \Rightarrow (|\Psi^{(i)}_{MP1} >, CMS \overset{SK_{CMS-MP}}{\longleftrightarrow} CMS)$

P25 is obtained on the basis of P24, A17 and R6 as:

P25: $MP| \equiv CMS| \equiv (MP \overset{sk}{\leftrightarrow} CMS)$ **[Goal 6]**

P26 is obtained on the basis of P25,A21 and R7 as:

P26: $CMS| \equiv GWN| \equiv (TS5, GWN \overset{Q7}{\longleftrightarrow} CMS)$

P27 is obtained on the basis of P26, A25 and R3 as:

P27: $CMS| \equiv GWN| \Rightarrow (CMS \overset{INFO_R}{\longleftrightarrow} MP)$

P28 is obtained on the basis of P27, R6 and A23 as:

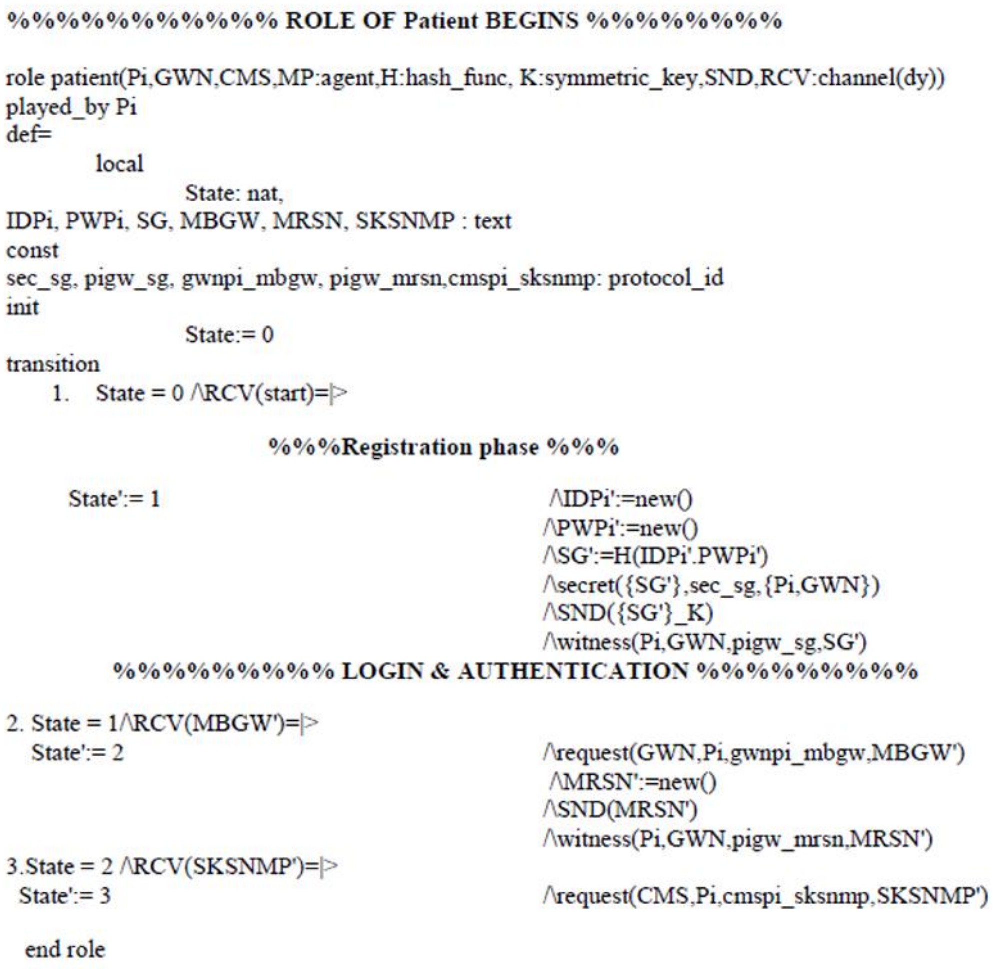
P28: $CMS| \equiv GWN| \equiv (CMS \overset{sk}{\leftrightarrow} GWN)$ **[Goal 4]**
P29 is obtained On the basis of P28, A21 and R1 as:
P29: $CMS| \equiv (CMS \overset{sk}{\leftrightarrow} GWN)$ **[Goal 3]**
According to message 4 and seeing the rule, we get the following:
P30: $MP \triangleleft (TS6, (GWN \overset{SK}{\longleftrightarrow} MP)_{INFO_R}$
P31 is obtained On the basis of P30, A21 and R1 as:
P31: $CMS| \equiv GWN| \Rightarrow (|\Psi_{GW-CMS} >, GWN \overset{Q7}{\longleftrightarrow} CMS)$
P32 is obtained on the basis of P31, A14 and R5 as:
P32: $CMS| \equiv (GWN \overset{QK}{\longleftrightarrow} MP)$
P33 is obtained On the basis of P32, A25 and R3 as:
P33: $CMS| \equiv GWN| \Rightarrow (TS6, CMS \overset{INFO_R}{\longleftrightarrow} MP)$
P34 is obtained on the basis of P33, A23 and R1 as:
P34: $GWN| \equiv MP| \equiv (GWN \overset{sk}{\leftrightarrow} MP)$ **[Goal 8]**
P35 is obtained on the basis of P34, A23 and R1 as:
P35: $GWN| \equiv CMS| \Rightarrow (CMS \overset{SK_{GW-CMS}}{\longleftrightarrow} GWN)$
P36 is obtained on the basis of P35, R6 and A28 as:
P36: $MP| \equiv SN| \equiv (MP \overset{sk}{\leftrightarrow} GWN)$ **[Goal 9]**

4.3.2 Simulation using AVISPA Tool

Following creating an authentication protocol, it is crucial to assess its security and validate its accuracy. Our protocol underwent simulation using the HLPSL language, along with the application of OFMC and CL-AtSe backends [22].

1. **HLPSL Specification**
   In the QSMAH protocol, the patient, GW node, CMS, and MP are represented as the patient, gw, cms, and mp, respectively. These are the four basic roles considered for HLPSL specification. The session and environment are the other two roles. In HLPSL, the user's role is represented in Figure 4.8. In the registration phase, the patient starts at State = 0 and receives the signal by transitioning from State = 0 → State'=1. In this transition, the patient generates identities as IDPi' and PWPi' using a new() operation. According to the new(), operation means these are fresh identities that have never been generated. It computes SG':= H(IDPi'.PWPi'). The statement secret ({SG'},sec_sg,{Pi, GWN}) means that SG' is secret and kept by Pi. The secrecy of SG' is represented by sec_sg: Protocol id. The patient sends ({SG'}_K) to GWN using the SND() operation. It also generates a statement as a witness (Pi, GWN,pigw_sg, SG'), which means SG' is generated as a fresh value by Pi to be shared with GWN. After registration in state =1, Pi receives {MBGW'} using RCV() operation. In the next transition, the Pi generates a statement as {GWN, Pi, gwnpi_mbgw, MBGW'} using the request operation for authentication by GWN. The patient also generates MRSN' as a fresh value and sends MRSN' to GWN using the SND command. The patient generates a statement as a witness (Pi, GWN, pigw_mrsn, MRSN'), which means SN authenticates this information. Once GWN authenticates SN, the session key between GWN and Pi is generated by GWN as {SKGWSN':= H(IDGW.IDSN')}.

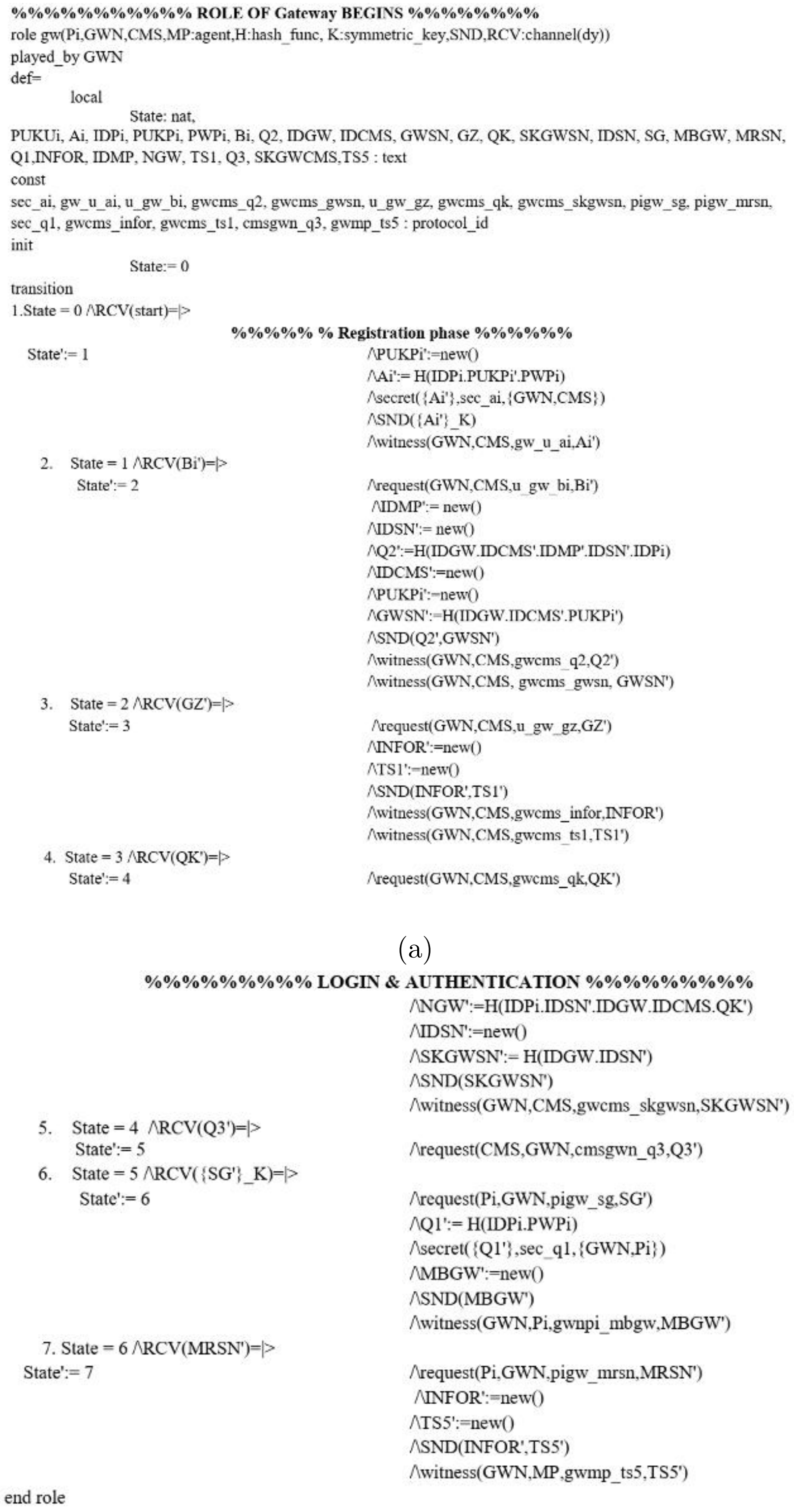
   Similarly, Figures, 4.9 and 4.10, and 4.11 specify the role of the Patient, GWN, CMS, and MP, respectively. The QSMAH goals and the specific roles of the session and environment are described in Fig.4.12 and 4.13. The specification roles for the patient as Pi, the Gateway as GW, and the Central Medical Server as CMS are the mandatory roles for the session and environment.



```
%%%%%%%%%%%% ROLE OF Patient BEGINS %%%%%%%%

role patient(Pi,GWN,CMS,MP:agent,H:hash_func, K:symmetric_key,SND,RCV:channel(dy))
played_by Pi
def=
        local
                State: nat,
IDPi, PWPi, SG, MBGW, MRSN, SKSNMP : text
const
sec_sg, pigw_sg, gwnpi_mbgw, pigw_mrsn,cmspi_sksnmp: protocol_id
init
                State:= 0
transition
    1.   State = 0 /\RCV(start)=|>

                         %%%Registration phase %%%

     State':= 1                                   /\IDPi':=new()
                                                  /\PWPi':=new()
                                                  /\SG':=H(IDPi'.PWPi')
                                                  /\secret({SG'},sec_sg,{Pi,GWN})
                                                  /\SND({SG'}_K)
                                                  /\witness(Pi,GWN,pigw_sg,SG')
            %%%%%%%%%% LOGIN & AUTHENTICATION %%%%%%%%%

2. State = 1/\RCV(MBGW')=|>
   State':= 2                                     /\request(GWN,Pi,gwnpi_mbgw,MBGW')
                                                   /\MRSN':=new()
                                                  /\SND(MRSN')
                                                  /\witness(Pi,GWN,pigw_mrsn,MRSN')
3.State = 2 /\RCV(SKSNMP')=|>
  State':= 3                                      /\request(CMS,Pi,cmspi_sksnmp,SKSNMP')

  end role
```

Figure 4.8: HLPSL code for the patient role in QSMAH protocol

2. **Simulation Results and Discussion**
   The implementation of QSMAH is performed using AVISPA(SPAN). The execution of the proposed protocol is under the OFMC and CL-AtSe backends. The OFMC ensures that legitimate entities can simulate the QSMAH protocol by considering a reply attack. The protocol also ensures that there is no passive intruder. The information about the sessions is also provided to the intruder by the backend. OFMC also verifies the possibility of an MITM attack. The verification is done by considering the intruder using Dolev-Yao model checking. Figure 4.14 represents simulation results for OFMC and CL-AtSe backend. The results reflect that the protocol is safe and secure. The simulation results provide results by verifying protocol is secure from active and passive attacks such as reply and MITM attacks.



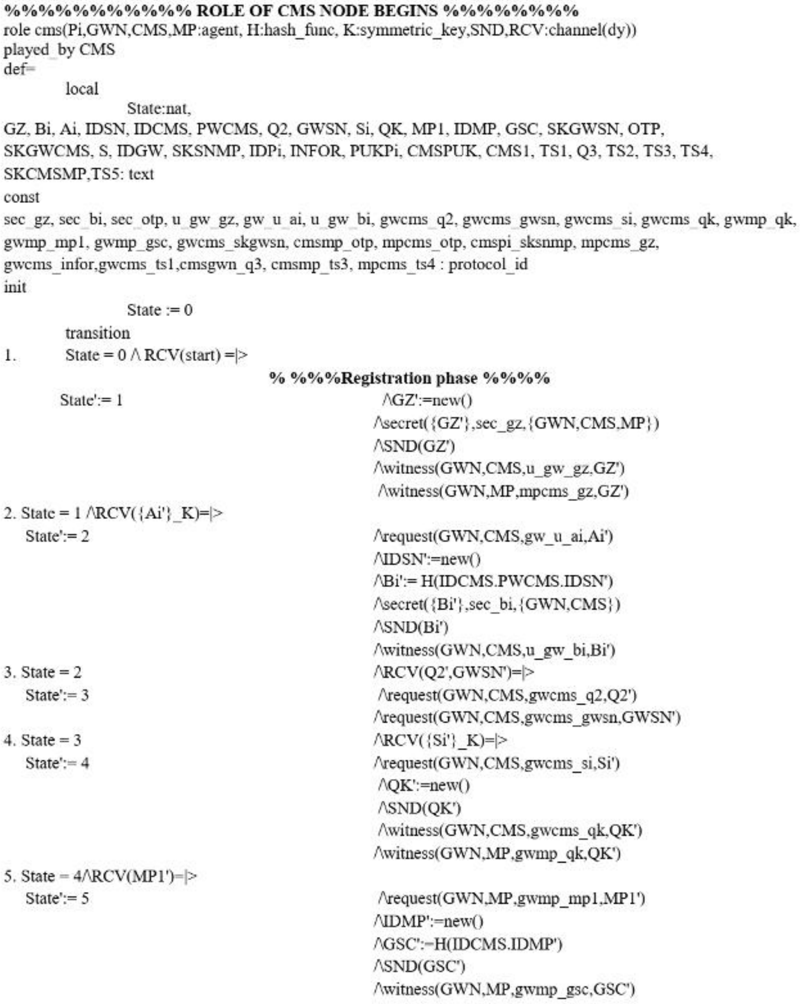
```
%%%%%%%%%%%% ROLE OF Gateway BEGINS %%%%%%%%
role gw(Pi,GWN,CMS,MP:agent,H:hash_func, K:symmetric_key,SND,RCV:channel(dy))
played_by GWN
def=
        local
                State: nat,
PUKUi, Ai, IDPi, PUKPi, PWPi, Bi, Q2, IDGW, IDCMS, GWSN, GZ, QK, SKGWSN, IDSN, SG, MBGW, MRSN,
Q1,INFOR, IDMP, NGW, TS1, Q3, SKGWCMS,TS5 : text
const
sec_ai, gw_u_ai, u_gw_bi, gwcms_q2, gwcms_gwsn, u_gw_gz, gwcms_qk, gwcms_skgwsn, pigw_sg, pigw_mrsn,
sec_q1, gwcms_infor, gwcms_ts1, cmsgwn_q3, gwmp_ts5 : protocol_id
init
                State:= 0
transition
1.State = 0 /\RCV(start)=|>
                                %%%%% % Registration phase %%%%%%
  State':= 1                                        /\PUKPi':=new()
                                                    /\Ai':= H(IDPi.PUKPi'.PWPi)
                                                    /\secret({Ai'},sec_ai,{GWN,CMS})
                                                    /\SND({Ai'}_K)
                                                    /\witness(GWN,CMS,gw_u_ai,Ai')
    2.   State = 1 /\RCV(Bi')=|>
          State':= 2                                /\request(GWN,CMS,u_gw_bi,Bi')
                                                     /\IDMP':= new()
                                                    /\IDSN':= new()
                                                    /\Q2':=H(IDGW.IDCMS'.IDMP'.IDSN'.IDPi)
                                                    /\IDCMS':=new()
                                                    /\PUKPi':=new()
                                                    /\GWSN':=H(IDGW.IDCMS'.PUKPi')
                                                    /\SND(Q2',GWSN')
                                                    /\witness(GWN,CMS,gwcms_q2,Q2')
                                                    /\witness(GWN,CMS, gwcms_gwsn, GWSN')
    3.   State = 2 /\RCV(GZ')=|>
         State':= 3                                  /\request(GWN,CMS,u_gw_gz,GZ')
                                                    /\INFOR':=new()
                                                    /\TS1':=new()
                                                    /\SND(INFOR',TS1')
                                                    /\witness(GWN,CMS,gwcms_infor,INFOR')
                                                    /\witness(GWN,CMS,gwcms_ts1,TS1')
    4.  State = 3 /\RCV(QK')=|>
         State':= 4                                 /\request(GWN,CMS,gwcms_qk,QK')
```

(a)

```
                 %%%%%%%%% LOGIN & AUTHENTICATION %%%%%%%%%
                                                      /\NGW':=H(IDPi.IDSN'.IDGW.IDCMS.QK')
                                                      /\IDSN':=new()
                                                      /\SKGWSN':= H(IDGW.IDSN')
                                                      /\SND(SKGWSN')
                                                      /\witness(GWN,CMS,gwcms_skgwsn,SKGWSN')
    5.   State = 4  /\RCV(Q3')=|>
          State':= 5                                  /\request(CMS,GWN,cmsgwn_q3,Q3')
    6.   State = 5 /\RCV({SG'}_K)=|>
          State':= 6                                  /\request(Pi,GWN,pigw_sg,SG')
                                                      /\Q1':= H(IDPi.PWPi)
                                                      /\secret({Q1'},sec_q1,{GWN,Pi})
                                                      /\MBGW':=new()
                                                      /\SND(MBGW')
                                                      /\witness(GWN,Pi,gwnpi_mbgw,MBGW')
    7. State = 6 /\RCV(MRSN')=|>
  State':= 7                                          /\request(Pi,GWN,pigw_mrsn,MRSN')
                                                       /\INFOR':=new()
                                                      /\TS5':=new()
                                                      /\SND(INFOR',TS5')
                                                      /\witness(GWN,MP,gwmp_ts5,TS5')
end role
```

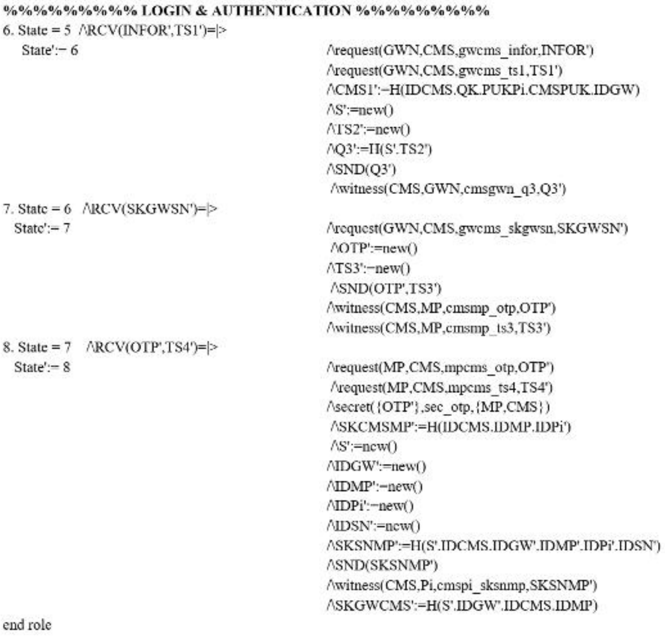
(b)

Figure 4.9: HLPSL code for role GWN in QSMAH protocol



```
%%%%%%%%%%%% ROLE OF CMS NODE BEGINS %%%%%%%%
role cms(Pi,GWN,CMS,MP:agent, H:hash_func, K:symmetric_key,SND,RCV:channel(dy))
played_by CMS
def=
        local
                State:nat,
GZ, Bi, Ai, IDSN, IDCMS, PWCMS, Q2, GWSN, Si, QK, MP1, IDMP, GSC, SKGWSN, OTP,
SKGWCMS, S, IDGW, SKSNMP, IDPi, INFOR, PUKPi, CMSPUK, CMS1, TS1, Q3, TS2, TS3, TS4,
SKCMSMP,TS5: text
const
sec_gz, sec_bi, sec_otp, u_gw_gz, gw_u_ai, u_gw_bi, gwcms_q2, gwcms_gwsn, gwcms_si, gwcms_qk, gwmp_qk,
gwmp_mp1, gwmp_gsc, gwcms_skgwsn, cmsmp_otp, mpcms_otp, cmspi_sksnmp, mpcms_gz,
gwcms_infor,gwcms_ts1,cmsgwn_q3, cmsmp_ts3, mpcms_ts4 : protocol_id
init
                State := 0
        transition
1.      State = 0 ∧ RCV(start) =|>
                                % %%%Registration phase %%%%
       State':= 1                                 ∧GZ':=new()
                                                  ∧secret({GZ'},sec_gz,{GWN,CMS,MP})
                                                  ∧SND(GZ')
                                                  ∧witness(GWN,CMS,u_gw_gz,GZ')
                                                  ∧witness(GWN,MP,mpcms_gz,GZ')
2. State = 1 ∧RCV({Ai'}_K)=|>
   State':= 2                                     ∧request(GWN,CMS,gw_u_ai,Ai')
                                                  ∧IDSN':=new()
                                                  ∧Bi':= H(IDCMS.PWCMS.IDSN')
                                                  ∧secret({Bi'},sec_bi,{GWN,CMS})
                                                  ∧SND(Bi')
                                                  ∧witness(GWN,CMS,u_gw_bi,Bi')
3. State = 2                                      ∧RCV(Q2',GWSN')=|>
   State':= 3                                     ∧request(GWN,CMS,gwcms_q2,Q2')
                                                  ∧request(GWN,CMS,gwcms_gwsn,GWSN')
4. State = 3                                      ∧RCV({Si'}_K)=|>
   State':= 4                                     ∧request(GWN,CMS,gwcms_si,Si')
                                                  ∧QK':=new()
                                                  ∧SND(QK')
                                                  ∧witness(GWN,CMS,gwcms_qk,QK')
                                                  ∧witness(GWN,MP,gwmp_qk,QK')
5. State = 4∧RCV(MP1')=|>
   State':= 5                                     ∧request(GWN,MP,gwmp_mp1,MP1')
                                                  ∧IDMP':=new()
                                                  ∧GSC':=H(IDCMS.IDMP')
                                                  ∧SND(GSC')
                                                  ∧witness(GWN,MP,gwmp_gsc,GSC')
```

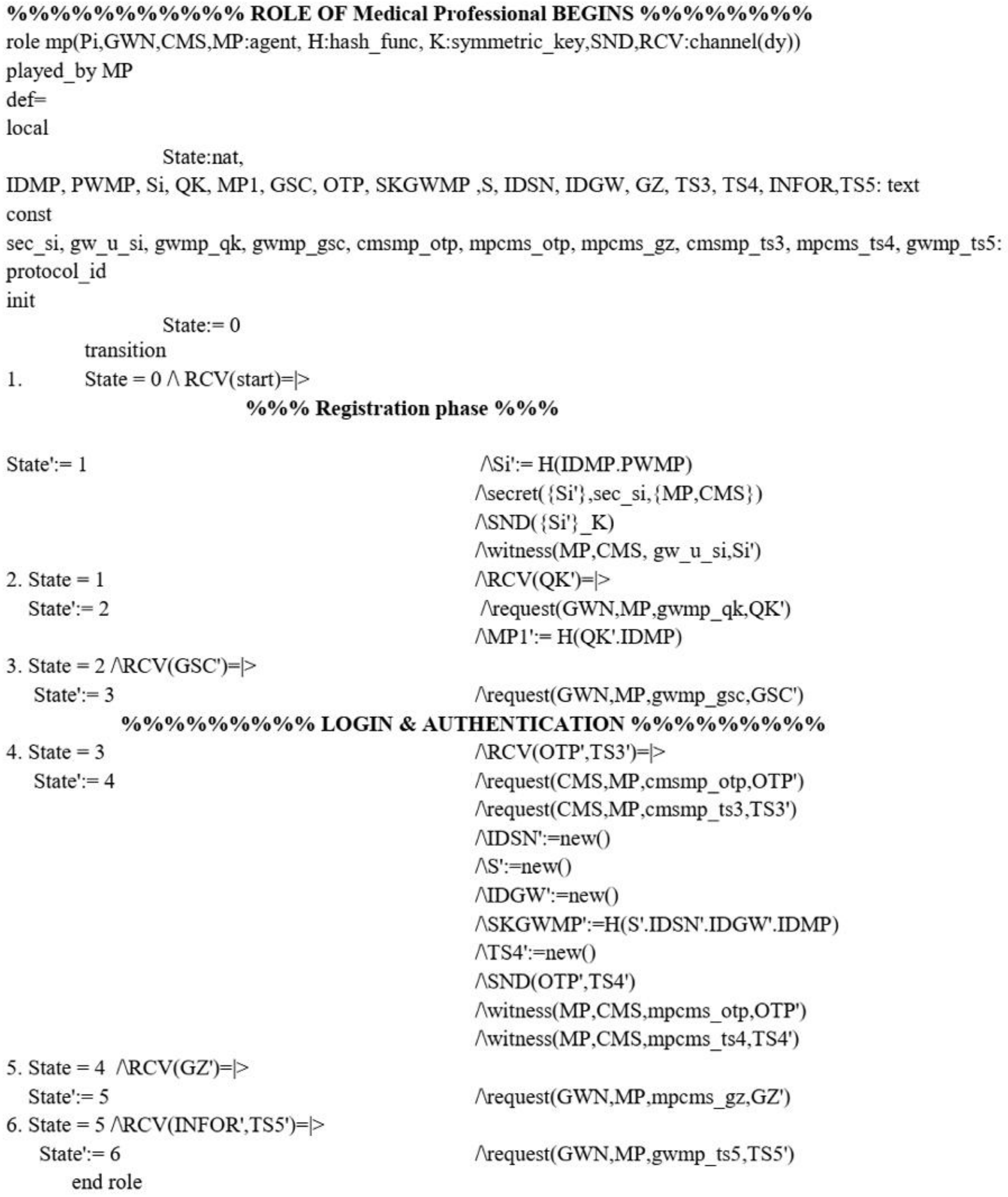
(a)



```
%%%%%%%%%% LOGIN & AUTHENTICATION %%%%%%%%%%
6. State = 5  ∧RCV(INFOR',TS1')=|>
   State':- 6                                  ∧request(GWN,CMS,gwcms_infor,INFOR')
                                               ∧request(GWN,CMS,gwcms_ts1,TS1')
                                               ∧CMS1':-H(IDCMS.QK.PUKPi.CMSPUK.IDGW)
                                               ∧S':=new()
                                               ∧TS2':=new()
                                               ∧Q3':=H(S'.TS2')
                                               ∧SND(Q3')
                                                ∧witness(CMS,GWN,cmsgwn_q3,Q3')
7. State = 6   ∧RCV(SKGWSN')=|>
  State':= 7                                   ∧request(GWN,CMS,gwcms_skgwsn,SKGWSN')
                                                ∧OTP':=new()
                                               ∧TS3':-new()
                                                ∧SND(OTP',TS3')
                                               ∧witness(CMS,MP,cmsmp_otp,OTP')
                                               ∧witness(CMS,MP,cmsmp_ts3,TS3')
8. State = 7   ∧RCV(OTP',TS4')=|>
  State':= 8                                   ∧request(MP,CMS,mpcms_otp,OTP')
                                                ∧request(MP,CMS,mpcms_ts4,TS4')
                                               ∧secret({OTP'},sec_otp,{MP,CMS})
                                                ∧SKCMSMP':=H(IDCMS.IDMP.IDPi')
                                                ∧S':=new()
                                               ∧IDGW':=new()
                                               ∧IDMP':-new()
                                               ∧IDPi':-new()
                                               ∧IDSN':=new()
                                               ∧SKSNMP':=H(S'.IDCMS.IDGW'.IDMP'.IDPi'.IDSN')
                                               ∧SND(SKSNMP')
                                               ∧witness(CMS,Pi,cmspi_sksnmp,SKSNMP')
                                               ∧SKGWCMS':=H(S'.IDGW'.IDCMS.IDMP)
end role
```

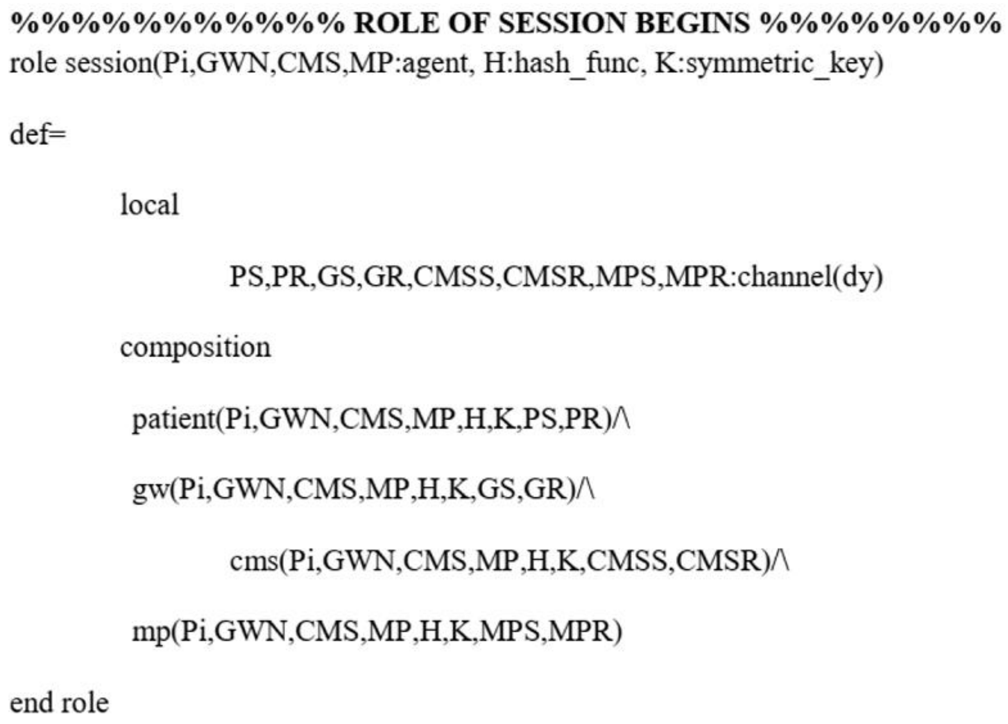
(b)

Figure 4.10: HLPSL code for role CMS in QSMAH protocol



```
%%%%%%%%%%%% ROLE OF Medical Professional BEGINS %%%%%%%%
role mp(Pi,GWN,CMS,MP:agent, H:hash_func, K:symmetric_key,SND,RCV:channel(dy))
played_by MP
def=
local
                State:nat,
IDMP, PWMP, Si, QK, MP1, GSC, OTP, SKGWMP ,S, IDSN, IDGW, GZ, TS3, TS4, INFOR,TS5: text
const
sec_si, gw_u_si, gwmp_qk, gwmp_gsc, cmsmp_otp, mpcms_otp, mpcms_gz, cmsmp_ts3, mpcms_ts4, gwmp_ts5:
protocol_id
init
                State:= 0
        transition
1.      State = 0 /\ RCV(start)=|>
                        %%% Registration phase %%%

State':= 1                                  /\Si':= H(IDMP.PWMP)
                                            /\secret({Si'},sec_si,{MP,CMS})
                                            /\SND({Si'}_K)
                                            /\witness(MP,CMS, gw_u_si,Si')
2. State = 1                                /\RCV(QK')=|>
   State':= 2                               /\request(GWN,MP,gwmp_qk,QK')
                                            /\MP1':= H(QK'.IDMP)
3. State = 2 /\RCV(GSC')=|>
   State':= 3                               /\request(GWN,MP,gwmp_gsc,GSC')
            %%%%%%%%%% LOGIN & AUTHENTICATION %%%%%%%%%%
4. State = 3                                /\RCV(OTP',TS3')=|>
   State':= 4                               /\request(CMS,MP,cmsmp_otp,OTP')
                                            /\request(CMS,MP,cmsmp_ts3,TS3')
                                            /\IDSN':=new()
                                            /\S':=new()
                                            /\IDGW':=new()
                                            /\SKGWMP':=H(S'.IDSN'.IDGW'.IDMP)
                                            /\TS4':=new()
                                            /\SND(OTP',TS4')
                                            /\witness(MP,CMS,mpcms_otp,OTP')
                                            /\witness(MP,CMS,mpcms_ts4,TS4')
5. State = 4  /\RCV(GZ')=|>
   State':= 5                               /\request(GWN,MP,mpcms_gz,GZ')
6. State = 5 /\RCV(INFOR',TS5')=|>
    State':= 6                              /\request(GWN,MP,gwmp_ts5,TS5')
      end role
```

Figure 4.11: HLPSL code for role MP in QSMAH protocol



```
%%%%%%%%%%% ROLE OF SESSION BEGINS %%%%%%%%
role session(Pi,GWN,CMS,MP:agent, H:hash_func, K:symmetric_key)

def=

          local

                    PS,PR,GS,GR,CMSS,CMSR,MPS,MPR:channel(dy)

          composition

           patient(Pi,GWN,CMS,MP,H,K,PS,PR)/\

           gw(Pi,GWN,CMS,MP,H,K,GS,GR)/\

                    cms(Pi,GWN,CMS,MP,H,K,CMSS,CMSR)/\

           mp(Pi,GWN,CMS,MP,H,K,MPS,MPR)

end role
```

Figure 4.12: HLPSL code for Session Role

4.3.3 Informal Security Analysis

Proposition 1. QSMAH achieves Mutual Authentication

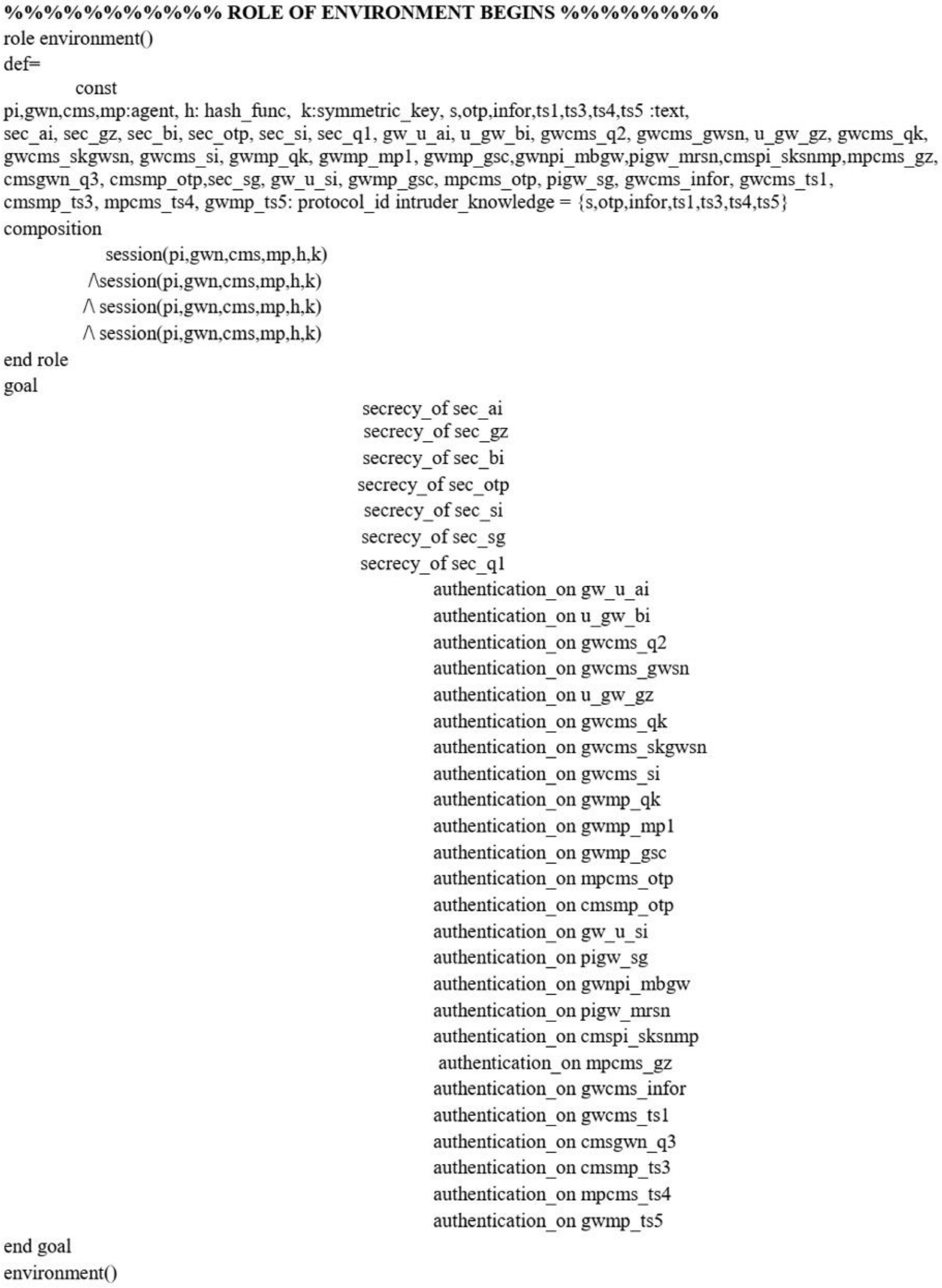
Proof: In the authentication process of QSMAH, CMS authenticates the MP by sending him {OTP, TS3} with an appropriate Time stamp. Authentication of the MP occurs when the OTP received by the CMS matches the sent OTP. As the OTP is delivered to the MP's communication device, such as their mobile phone, it remains inaccessible to adversaries. CMS authenticates the GWN by receiving $INFO_R$ based on which he can retrieve: $Q2 = h(ID_p||ID_{SN_i}||ID_{GW}||ID_{MP})$ and verify ID_{GW}.

Proposition 2. QSMAH achieves Patient, GWN, CMS, and MP anonymity

Proof: To conceal the identity of the Patient, GWN, CMS, and MP, the information pertinent to their identification is stored secretly using OWHF (Q1, Q2, Q3, Q4, Q5, Q6, Q7). Additionally, the patient Body Sensor Node(BSN) identities are shared as encoded information with CMS. If an intruder intercepts messages from the Patient, GWN, CMS, and MP, they won't be able to determine identities such as ID_p, ID_{SN_i}, ID_{GW} and ID_{MP}. The distinct identities are concealed and secured using OWHF in communication messages.

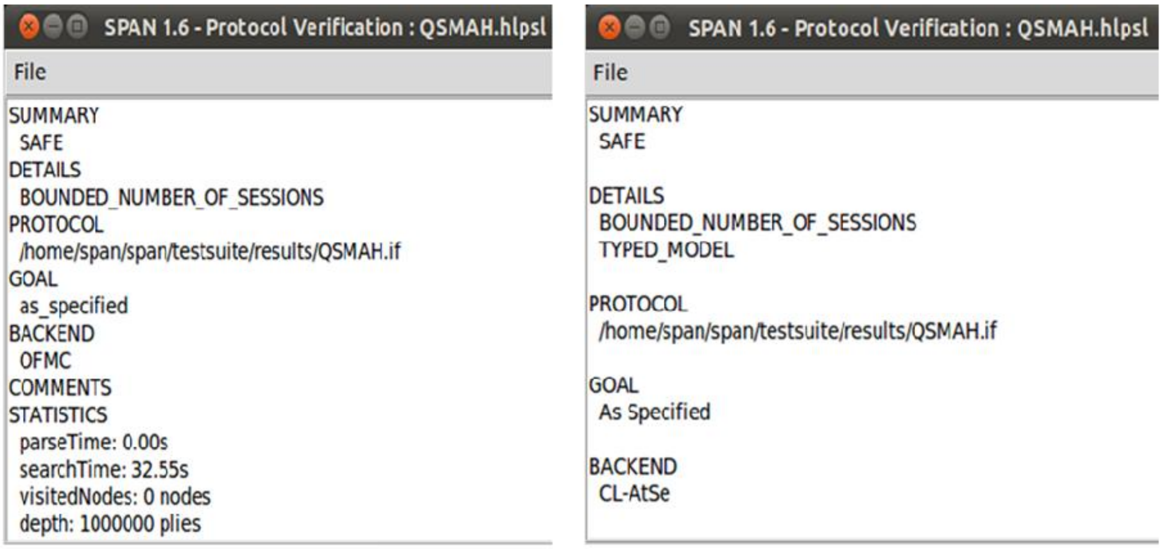
Proposition 3. QSMAH resists replay attack

Proof: It is presumed that in QSMAH, a global clock is maintained for time synchro-



```
%%%%%%%%%%%%% ROLE OF ENVIRONMENT BEGINS %%%%%%%%%
role environment()
def=
        const
pi,gwn,cms,mp:agent, h: hash_func,  k:symmetric_key, s,otp,infor,ts1,ts3,ts4,ts5 :text,
sec_ai, sec_gz, sec_bi, sec_otp, sec_si, sec_q1, gw_u_ai, u_gw_bi, gwcms_q2, gwcms_gwsn, u_gw_gz, gwcms_qk,
gwcms_skgwsn, gwcms_si, gwmp_qk, gwmp_mp1, gwmp_gsc,gwnpi_mbgw,pigw_mrsn,cmspi_sksnmp,mpcms_gz,
cmsgwn_q3, cmsmp_otp,sec_sg, gw_u_si, gwmp_gsc, mpcms_otp, pigw_sg, gwcms_infor, gwcms_ts1,
cmsmp_ts3, mpcms_ts4, gwmp_ts5: protocol_id intruder_knowledge = {s,otp,infor,ts1,ts3,ts4,ts5}
composition
            session(pi,gwn,cms,mp,h,k)
          /\session(pi,gwn,cms,mp,h,k)
          /\ session(pi,gwn,cms,mp,h,k)
          /\ session(pi,gwn,cms,mp,h,k)
end role
goal
                        secrecy_of sec_ai
                        secrecy_of sec_gz
                        secrecy_of sec_bi
                        secrecy_of sec_otp
                        secrecy_of sec_si
                        secrecy_of sec_sg
                        secrecy_of sec_q1
                            authentication_on gw_u_ai
                            authentication_on u_gw_bi
                            authentication_on gwcms_q2
                            authentication_on gwcms_gwsn
                            authentication_on u_gw_gz
                            authentication_on gwcms_qk
                            authentication_on gwcms_skgwsn
                            authentication_on gwcms_si
                            authentication_on gwmp_qk
                            authentication_on gwmp_mp1
                            authentication_on gwmp_gsc
                            authentication_on mpcms_otp
                            authentication_on cmsmp_otp
                            authentication_on gw_u_si
                            authentication_on pigw_sg
                            authentication_on gwnpi_mbgw
                            authentication_on pigw_mrsn
                            authentication_on cmspi_sksnmp
                            authentication_on mpcms_gz
                            authentication_on gwcms_infor
                            authentication_on gwcms_ts1
                            authentication_on cmsgwn_q3
                            authentication_on cmsmp_ts3
                            authentication_on mpcms_ts4
                            authentication_on gwmp_ts5
end goal
environment()
```

Figure 4.13: HLPSL Role of Environment of QSMAH


SPAN 1.6 - Protocol Verification : QSMAH.hlpsl
File

```
SUMMARY
 SAFE
DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
 /home/span/span/testsuite/results/QSMAH.if
GOAL
 as_specified
BACKEND
 OFMC
COMMENTS
STATISTICS
 parseTime: 0.00s
 searchTime: 32.55s
 visitedNodes: 0 nodes
 depth: 1000000 plies
```

SPAN 1.6 - Protocol Verification : QSMAH.hlpsl
File

```
SUMMARY
 SAFE

DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
 TYPED_MODEL

PROTOCOL
 /home/span/span/testsuite/results/QSMAH.if

GOAL
 As Specified

BACKEND
 CL-AtSe
```

Figure 4.14: Simulation results of QSMAH using OFMC and CL-AtSe backend

nization. The entire information is communicated using TS. Even if the adversary can capture the TS, he may not be able to generate the same hash value as $h(S||TS2||ID_{GW})$ due to insufficient information.

Proposition 4. QSMAH provides Forward secrecy

Proof: In QSMAH, the Patient, CMS, and MP share different session keys:SK_{GW-SN}, SK_{CMS-MP}, SK_{GW-CMS}. These session keys are random and generated after login and authentication. Therefore, an adversary can't forge session keys. The Quantum information cannot be copied due to the No-cloning principle; therefore, storing the intermediate information to generate the session key later is impossible.

Proposition 5: QSMAH provides privileged insider attack

Proof: In this proposed protocol, assume that the malicious insider can retrieve information such as ID_{MP} and ID_{CMS}. However, even if he gets Patient or MP credentials, he may not be able to generate OTP. OTP is delivered only to registered authenticated devices during the pre-deployment phase. The maximum time limit of OTP is 5 minutes. Therefore, it is challenging for a malicious insider to perform calculations efficiently.

Proposition 6: QSMAH provides Secret Key security

Proof: In the QSMAH protocol, after MA, the session key is generated SK_{SN-MP}. It is generated after intermediate session keys as SK_{GW-CMS} and SK_{GW-MP}. It is unachievable for an intruder to generate the intermediate session keys with OWHF as $SK_{SN-MP} = h(S||ID_{GW}||ID_{CMS}||ID_P||ID_{MP})$.

Proposition 7: QSMAH ensures Secret Key communication

Proof: In the QSMAH protocol, instead of classical key generation, which is generated by one entity and communicated with others using the insecure channel. In our protocol, the Quantum key based on rand basis is generated by each identity as $Q_{k_H} = k^u_{MP} \bigoplus K^u_p$ and $Q_{k_H} = k^u_{MP} \bigoplus K^u_{CMS}$. Based on this, the final key is generated and accepted by each communicating entity as $Q_{k_H} = k^u_{CMS} \bigoplus K^u_{MP} \bigoplus K^u_p$.

Proposition 8: QSMAH ensures Entanglement security

Proof: In the proposed protocol, the entities correlate with each other using the process of Quantum Entanglement. The authentication process runs on GHZ state as the state is initially shared with legitimate devices only even before the registration starts. However, even if the adversary can receive one device's information, he can't retrieve the information generated by other entities.

Proposition 9: QSMAH ensures Information Teleportation

Proof: In the proposed protocol, the information transfer using the process of Quantum teleportation is as $|\Psi>_{GWSN} = Q2 \bigotimes |0>_{GHZ}$. Even if the adversary can receive the information as $INFO_R$, it is practically impossible that he may guess the information to be generated by other entities(CMS, MP, GWN) due to Quantum Unitary gates.

Proposition 10: QSMAH defends against MITM attack

Proof: The suggested protocol is protected against Man-in-the-Middle (MITM) attacks. If the adversary tries to intercept $Q7 = h(S||ID_p||ID_{GW}||ID_{MP})$.

It cannot impose active or passive attacks. An adversary can't extract secure identities by using OWHF.

4.4 Results and Discussion

In this section, we address the technical hurdles of the proposed scheme. Subsequently, we evaluate its efficiency and examine the security threats the proposed QSMAH protocol mitigated.

4.4.1 Technical Challenges

1. **Quantum Entanglement**
   In our proposed protocol, Quantum computation information is shared between communicating entities by establishing an EPR pair. These pairs are distributed between the remote nodes. However, the decay of entanglement is reported as a function of distance. Many efforts have also been taken to mitigate the effects of decoherence in entanglement sharing. However, further research is needed from a network designer's perspective.

2. **Maximum Distance for Successful QKD Transmission**
   Long distances Quantum communication is an important research issue. The challenge is due to the regeneration of the Quantum signal. The overall maximum distance covered by QKD transmissions is currently over 200 km, successfully implemented. Additionally, the bit rate of QKD systems reaches only a few Mbit/s in a telecom metropolitan area network. Still, this disturbance is too high beyond 50 kilometres, which increases error rates. Therefore, it leaves the channel vulnerable to eavesdroppers and makes it virtually impossible to send information[167].

3. **Cost-effective**
   Considering the recent advances in Quantum machines, due to the high cost, it is impractical to use them for applications such as health care where large numbers of sensor nodes are deployed to monitor patient medical conditions. In such a framework, using Quantum machines as nodes is challenging due to high cost, dimensions, and stability conditions. Recently, researchers have focused on developing cost-effective Quantum sensors that could be deployed in required smart applications.

4.4.2 Efficiency Analysis

1. **Quantum Parallelism:**
   In our protocol, the GHZ state allows parallel Quantum computation by entangling multiple Qubits. Each Qubit in a GHZ state can be in a superposition of state, allowing for parallel processing of multiple Qubits. To achieve Quantum parallelism in our work, we have used IBM Quantum Experience (IQE), which will explore many computational paths in a shorter period than classical computers.

2. **Quantum Network:**
   Our protocol allows the transfer of Quantum states between different nodes in a network. Such information is transferred securely without physically transmitting Quantum particles over long distances by implementing the process of Quantum teleportation. This contributes to enhancing the efficiency of the proposed scheme.

3. **Key distribution efficiency:**
   QKD schemes can generate secure cryptographic keys at high rates and allow efficient key establishment. Additionally, by taking advantage of the Quantum Mechanics principle, any eavesdropping on the key exchange can easily be detected.

4. **Quantum Superposition:**
   In QSMAH, qubits are used for quantum communications. Such Qubit exists in 0 and 1 or any superposition (i.e. both 0 and 1 states simultaneously). As we implemented QSMAH on IBM Quantum Experience (IQE), such Quantum computers can access potentially large computational space. Such ability makes Quantum computers powerful. A classical computer with n bits can perform a maximum of N calculations at once. However, Quantum computers can manage up to 2^n operations [168]. For example, if a classical system can perform 5 operations, a Quantum computer can perform $2^5 = 32$ operations simultaneously. This will allow the proposed protocol efficiency to outperform classical information processing.

4.4.3 Discussions on Attacks

1. QSMAH is resistant to Forward Secrecy attack
   Proof: Assume even if the adversary can intercept the session key as $SK_{GWSN} = h(M_R||ID_{GW}||ID_{SN_i})$, still he may not be able to access complete information from the session As M_R is impossible to extract. QSMAH also ensures that a different Quantum state is produced in each step, ensuring that no information leakage is possible.

2. User Impersonation Attack
   Proof: Consider an attacker A by using the patient's Mobile phone, can get his $h(ID_p||PW_p)$ and can verify the information stored in GWN. He may also acquire $h(P_{puk})$ of the user and can verify it. By generating other information from the patient's Mobile, he may be able to generate successfully: $Q2 = h(ID_p||ID_{SN_i}||ID_{GW}||ID_{MP})$. However, the attacker may not be able to get complete $|\emptyset >_{GHZ}$ and therefore not able to identify what information CMS and MP obtain when they receive $\{c_1, c_0\}$ as $INFO_R$.

3. Stolen smart card attack
   Proof: Assume that attacker A infers the MP QGC as $|\Psi^{(i)}_{CMS2} >, |\Psi^{(i)}_{MP1} >, CMS_{pui}, |\phi^{(i)}_{GHZ} >$. Using this information, he may be unable to extract the complete user details. As the information is in the superposition of the state using which he may only be able to perceive classical information, such as CMS_{pui}.The attacker may not be able to guess $|ID_{MP} >, |PW_{MP} >$ due to the superposition of the state.

4. Sensor impersonation attack
   Proof: Let's consider an intruder who successfully obtains the $|ID_p >$ and $|PW_p >$ by accessing patient information from the server. The attacker may try to impersonate an actual BSN and inject false data into the network. However, QSMAH does not allow the adversary to send false information to GWN by using Quantum error correction Pauli gates $\{|+ >\rightarrow I, |- >\rightarrow Z\}$ for $|CW_{SN} >$.

5. Traffic analysis
   Proof: Considering an attacker A may try to capture the Quantum secret keys to be shared between GWN, CMS, and MP as $Q_{k_H} = k^u_{CMS} \bigoplus K^u_{MP} \bigoplus K^u_p$.To generate the Quantum key, he may able to generate accurately Q_{CMS_k}, Q_{MP_k} and Q_{GW_k}. It is impossible for attacker A to predict the intermediate information on an accurate basis. Therefore, QSMAH ensures resistance to traffic analysis attacks.

6. Safe from GWN bypassing attack
   Proof: Assume an attacker A may try to bypass GWN. Our protocol is safe against this attack. As GWN may encode secret information as $|\phi >_{GWSN} = Q2 \bigotimes |\emptyset >_{GHZ}$ and generate $\{c_1, c_0\}$ as $INFO_R$.GWN is responsible for running the authentication step between patient, CMS, and MP.

7. GWN Impersonation
   Proof: An intruder may try to impersonate a legitimate GWN. The CMS is an authenticated entity with a list of registered GWNs. The Quantum state encoded by GWN as $|\phi >_{GWSN}= Q2\bigotimes|\emptyset >_{GHZ}$. Based on which CMS could verify legitimate GWN.

8. Quantum Attack
   Proof: The QSMAH is based on Quantum laws. The process of Quantum teleportation, which sends the encoded information $|\phi >_{GWSN}= Q2\bigotimes|\emptyset >_{GHZ}$ as $INFO_R$.To be generated by CMS and make our protocol Quantum resistance.

9. Key Exchange Attack
   Proof: Considering an external intruder, I may try to capture the private keys communicated over classical channels. However, the authentication is based on the Quantum key agreement $Q_{k_H} = k^u_{CMS}\bigoplus K^u_{MP}\bigoplus K^u_p$.It is generated individually by mutual coordination between legitimate entities.

10. MITM attack
    Proof: Assume an attacker A may capture $Q2 = h(ID_p||ID_{SN_i}||ID_{GW}||ID_{MP})$ generated by GWN. He may try to change the identities, such as ID_{MP} and ID_{GW}. However, he will not be able to encode the state Q2 as $|\phi >_{GWSN}= Q2\bigotimes|\emptyset >_{GHZ}$.It is impossible for an attacker to generate a GHZ state.

11. Session key agreement
    Proof: Assume an attacker A may try to generate SK_{GW-CMS} .However, he may not be able to verify that the hash value that he has generated is equivalent to $h(S||ID_{GW}||ID_{CMS})$.

12. Resist DoS attack
    Proof: Assume an attacker A may try to execute a DoS attack against CMS. The adversary may try to login with fake credentials. However, in our protocol, the attacker may not be able to produce $|ID_p >$ as this is in the superposition of state. The second case is also impossible CMS checks the Time stamps as TS1, TS2, and TS4.

4.5 Summary

This chapter reviews the existing healthcare IoT authentication protocols that suffer from many classical and futuristic Quantum Computing attacks. As analyzed with the advancement in Quantum computing, it is impossible to maintain a high-level secured framework for healthcare in IoT applications using classical cryptographic schemes. Therefore, we proposed a QSMAH protocol that ensures KA and MA for healthcare in IoT systems. The novelty of our work is based on the proposed modified QKD scheme and unique properties of GHZ states for achieving authentication for healthcare in IoT. In our protocol, instead of using the classical channel for sharing information, the secret information is shared through Quantum Teleportation based on maximally entangled states. Hence, the QSMAH protocol resists Classical as well as Quantum attacks. The formal proof using BAN logic is analyzed. The proof reflects that the security requirement that must be considered is satisfied. We employ the AVISPA tool for simulating QSMAH to verify the safety and security of our protocol. Informal security analysis demonstrates that the proposed protocol is resilient against real-time attacks, including replay and Man-in-the-Middle (MITM) attacks.

Chapter 5

ANALYSIS of QUANTUM-BASED SCHEMES FOR IoT

5.1 Introduction

The connectivity of IoT applications through the internet has provided a futuristic vision of connected living. The Quantum Computer running Shor's algorithm with stable 4099 qubits can break RSA-2048 encryption in 10 seconds. Most of the internet security today relies on public key cryptography. The public key encryption algorithms used today are RSA, DSA, DH, ECDH, and ECDSA. Organizations such as the military, banks and security organizations want to keep their data secure and confidential for the long term, say, 25 years. These organizations require adopting Quantum Cryptography techniques. In this chapter, we analyze the Quantum schemes concerning IoT security. We also discuss the classical mutual authentication schemes and their comparison with Quantum schemes for resource-constrained IoT.

5.2 Analysis of Quantum Schemes in IoT

5.2.1 Quantum Systematic Analysis

The authors[125, 146] discussed the drawbacks of classical encryption techniques and discussed Quantum Computing that employs a flow of photons for data transmission. These photons possess a characteristic called ”spin.” There exist four fundamental spin orientations: horizontal, vertical, 45-degree diagonal and negative 45-degree diagonal. In the realm of physics, the Heisenberg uncertainty principle is a captivating concept, asserting that it is extremely challenging to precisely measure all the attributes of a particle without causing a disturbance to its existing state. The recent impact of Quantum on IoT security, followed by 5G-enabled IoT security concerns and by exploiting backwards-interoperability aspects of the 5G security system, has also been discussed[72]. However, the author is unable to provide light on new cryptographic protocols which can resist Quantum attacks. Furthermore, the pursuit of data security dates back to the Spartan era, and today, unmanned aerial vehicles (UAVs) are gaining widespread popularity across various fields like agriculture, military and versatile mobility. Through an examination[7], the paper sheds light on current security challenges in real-world scenarios and underscores the significance of Quantum Cryptography in safeguarding information compared to conventional solutions. The authors discussed the role of Quantum coin flipping, Quantum commitment, and Position-based Quantum Cryptography for secure UAV authentication.

As we enter a new decade, Intelligent Infrastructure (II) services seamlessly integrated into the Internet of Things (IoT) are advancing technologically. The authors [125] discussed that most existing public key cryptography (PKC) methods are susceptible to possible threats from Quantum computers. Post-quantum cryptography (PQC) provides remedies to counter these threats. In the current Internet age, sensitive information is often sent over insecure channels. Given the substantial advancements in Quantum Computing, there's a demand for absolute security in safeguarding confidential data. Quantum key distribution protocols are established as secure as long as all the devices involved are flawless [126]. Therefore, Quantum Key distribution protocols based on the Heisenberg Uncertainty principles, such as BB84, BB92, SARG04, Six-State protocol and Quantum Entanglement based, such as E91 protocol, COW and DPS protocols, are discussed by Kumar et al. [126].

Considering the necessity of Quantum Cryptography for future internet-based security, Chawla et al.[77] recently proposed a survey to establish a structured guide in the realm of Quantum-secured IoT communication within the context of 5G. This guide will encompass the latest research on 5G-enabled IoT, including its pivotal enabling technologies, the potential risks faced by 5G-enabled IoT applications, and the most advanced quantum-based solutions and initiatives available.

In our work, an in-depth analysis of Quantum Cryptography for resource-constrained IoT considering the 5G-enabled IoT security concerns, an in-depth analysis of classical authentication-based schemes, a thorough investigation of Quantum Cryptography for IoT framework, an analysis of Post-Quantum Cryptography and the comparison of Quantum Cryptography and Post Quantum Cryptography has been provided.

5.2.2 Quantum Authentication Protocols

We provide insight to the readers about how Quantum Cryptography has proven to be a prominent technology for solving security concerns in IoT. Currently, IoT objects are extensively used and provide many benefits to the user. V et al. [168] discussed quantum-based authentication for securing healthcare data. The suggested approach relies on the following steps: a) Converting random numbers into the required set of Qubits. b) Sharing the qubits between sender and receiver by considering the random basis. c) Comparison is performed to generate the final key. The proposed protocol is proven secure compared to classical authentication schemes such as RSA, ECC and AES. However, authentication in the healthcare scenario is not thoroughly investigated. To secure the banking transactions, the authors proposed the idea of a Quantum cheque [150]. The authors secure the cheque amount by securely generating and distributing the BB84 Quantum key. The authors proposed the Quantum locker for securing the messages. The proposed scheme is based on generating the Quantum password. The scheme lacks the authentication model for securing data generated from entities. Considering the drawbacks of the authentication protocol, Chawla et al.[169] protocol comprises five steps such as a) **Preparation phase:** During this stage, each participant within the communication network is assigned a distinct identifier. Furthermore, these entities must be able to generate both asymmetric and symmetric keys. b) **Gen Algorithm:** In this step, entities create maximally entangled states among themselves, including GWN, Medical server, and Professionals, as in Eq.5.1:

$$|\psi^{\pm}_{0,0\bigoplus r,0\bigoplus u}>_{ABC}=\frac{1}{\sqrt{2}}(|0,0\bigoplus r,0\bigoplus u>+|1,1\bigoplus r,1\bigoplus u>) \tag{5.1}$$

Registration Algorithm: In this step, the patient initiates registration with the Medical server using their mobile device (GWN). Medical professionals also complete their registration with the Medical server through the Gateway. The GWN validates the registration information for authentication and subsequently shares this data with the Medical server to ensure secure future logins.

1. **Patient Registration:** In this, the patient's secret credentials are encoded as in Eq.5.2:

$$|\phi >_{GWSN}= Q2 \bigotimes |\emptyset >_{GHZ} \tag{5.2}$$

   Where, $Q2 = h(ID_p||ID_{SN_i}||ID_{GW}||ID_{MP})$. Such information is securely transferred using a Quantum teleportation channel to authenticated entities.

2. **Medical Professional registration:** Each medical professional must register onto the Medical server by sharing the credentials such as $Q3 = h(ID_p||PW_p)$. The medical professional gets registered on the Medical server by generating the Quantum Green Health Card (QGHC).

3. **Login Algorithm:** During this step, the authorised patient securely accesses the system to request medical advice from a certified physician.

4. **Authentication Algorithm:** In this stage, the patient, Medical Server (MS), and Medical Professional (MP) mutually authenticate themselves over a secure Quantum channel. Each user must be securely login into the system by decrypting $|\phi >_{GWSN}= Q2 \bigotimes |\emptyset >_{GHZ}$. To secure the data from any unauthorized entities, a modified Quantum key approach has been adopted as in Eq.5.3

$$QK : k_{MP} \bigoplus k_p \bigoplus k_{CMS} \tag{5.3}$$

   The proposed protocol is for resource-constrained IoT devices. Quantum gates such as X and Z, Hadamard and CNOT effectively realise the proposed scheme. The secure generation of GHZ states allows only authenticated entities to retrieve the data.

5.3 Security analysis

In this section, we present how the Quantum-enabled protocol QSMAH fulfils nearly all the prerequisites for securing resource-constrained IoT communication, while others fall short in achieving some aspects, as detailed in Table 5.1.

(a) **Replay Attack :** This occurs when the opponent intercepts user credentials and transmits them to the server via the authenticated channel. Nonetheless, Quantum No Cloning prevents the duplication of user information.

(b) **MITM attack:** In this scenario, the attacker intercepts network data to access information. By appropriating the transmitted messages, the attacker creates an illusion of direct communication between users while contaminating the conversation. However, using Quantum principles eavesdropping could be easily identified.

Table 5.1: Comparison of the security feature of Quantum with other authentication protocols

Security Consideration	[144]	[170]	[171]	[118]	[102]	[168]	[169]
Replay attack	✓	✓	-	-	-	-	✓
MITM attack	-	✓	-	-	✓	✓	✓
DoS attack	-	✓	-	-	-		✓
Key Exchange Attack	-	-	-	✓	-	✓	✓
GWN Impersonation	✓	-	-	-	-	-	✓
Traffic Analysis	-	-	-	-	-	-	✓
Sensor Impersonation	✓	-	-	-	-	-	✓
User Impersonation	-	✓	-	✓	✓	-	✓
Mutual Authentication	-	-	-	✓	-	-	✓

(c) **GWN Impersonation:** To thwart an attacker's attempt to intercept transmitted messages from a GWN (Gateway Node), it is imperative to employ an authenticated gateway node.

(d) **Denial of Service (DoS):** A Denial of Service (DoS) attack can be illustrated by envisioning a situation in which an assailant inundates the target with excessive traffic to seize and entirely exhaust its memory resources.

(e) **Key Exchange Attack:** By using Quantum Key Distribution such as BB84, any eavesdropping in key generation and distribution can easily be identified based on the probability of the outcome received.

(f) **User Impersonation Attack:** In a given situation, adversaries transmit user information to the gateway. By falsifying user credentials, the adversary convinces the GWN that the message originates from an authenticated user. By using entanglement between entities, it is impossible to perform this attack.

(g) **Sensor Impersonation Attack:** This scenario occurs when the adversary obtains confidential sensor data and then impersonates the legitimate user on the server. Quantum entanglement and Quantum gates make this attack impossible.

(h) **Traffic Analysis:** The assailant eavesdrops on network communications with the intention of discerning patterns in application behaviour, the configuration of routing, the positions of critical nodes, and the locations of base stations.

5.4 Summary

This section outlines IoT security concerns and the necessity of Quantum-enabled solutions for a secure IoT communication framework. Therefore, we discuss Quantum-enabled schemes for resource-constrained IoT communication frameworks and compare various Quantum-enabled schemes with classical authentication protocols.

Chapter 6

CONCLUSION AND FUTURE SCOPE

6.1 Conclusion

Our work is primarily motivated by examining the intricate and crucial security needs associated with IoT communication. IoT frameworks can potentially connect with numerous devices and objects using the Internet, leading to serious security issues. In such an environment, eavesdroppers may gain entry to the network communication by executing data breaches and false node injection attacks. Such systems have relied on AES, RSA, hashing, and ECC schemes to ensure security. Quantum Computing threatens classical cryptographic schemes. Therefore, considerable research is required to prepare the Quantum-enabled framework for securely transferring patient data among IoT devices. In this thesis, we propose two Quantum cryptography-based Mutual Authentication schemes for a secure IoT-enabled communication framework:

1. QAKA: Novel Quantum Authentication and Key Agreement protocol
2. QSMAH: Novel Quantum-based Secure Cryptosystem using Mutual Authentication for Healthcare

In Chapter 2, we first examined the necessity of secure IoT communication, given the increasing popularity of IoT devices in conjunction with high-speed 5G internet connectivity. The cryptographic analysis of safe and sound IoT communication needs to be addressed. Therefore, we examined the recent forge ahead in Quantum computing to yield a promising future in data and network security. Quantum cryptography-based QKD protocols can solve cyberspace security and key exchange issues for future secure internet communication. In Chapter 3, we have presented the novel secure Key Agreement (KA) and Mutual Authentication (MA) scheme based on Quantum Cryptography for a secure IoT communication framework. The proposed scheme is based on the states of QKD and GHZ. Secure Key distribution is based on BB84 protocol. We present the four particle GHZ states on IBM Quantum Experience(IQE) for MA and secure data transfer. The mutual authentication (MA) among the user, GWN, and QSN is established through widely acknowledged Burrows, Abadi, and Needham (BAN) logic. Formal verification of the proposed scheme's security is demonstrated using the Random Oracle Model (ROM) and Automated Validation of Internet Security Protocols and Applications (AVISPA). A thorough security examination indicates the proposed scheme is resilient against classical and potential future Quantum attacks. The performance of the proposed protocol is presented, revealing superior efficacy when compared with classical authentication schemes and Quantum protocols.

In Chapter 4, we discussed the recently proposed mutual authentication schemes for securing IoT-based healthcare data suffer from classical and futuristic Quantum threats. Therefore, for the secure transfer of patient data through CMS to MP QSMAH protocol is presented. The proposed scheme ensures Secret Key Distribution and MA based on modified QKD and generated GHZ states. We have implemented the three-particle GHZ state on IBM Quantum Experience (IQE). The AVISPA tool simulates the suggested approach (i.e., QSMAH). The examination of the results confirms the robustness and safety of the protocol. Extensive formal security assessment using BAN logic validates the protocol's security objectives. An informal analysis highlights its effectiveness in achieving secure key distribution and mutual authentication. The outcomes demonstrate the protocol's immunity to tampering by Quantum Shor's and Grover's algorithms and its resilience against classical attacks such as MITM, user anonymity, and impersonation attacks.

In Chapter 5, we have presented the comparative analysis of Quantum and Classical schemes. The outcomes indicate that the presented approaches fulfil all the security requirements for IoT devices with limited resources.

6.2 Future Scope

In this section, we explore that our proposed research provides many new dimensions worth exploring in future work.

1. **Cloud Security:**
   In the context of IoT, heightened attention to security measures becomes imperative when dealing with the storage and processing of information in the Cloud environment. This is particularly crucial as IoT devices often rely on cloud-based platforms to manage and analyze data, demanding comprehensive security considerations to protect the confidential data of the IoT ecosystem.

2. **AWS Braket:**
   When implementing Quantum-based authentication protocols, it becomes essential to underscore the significance of heightened security measures. Specifically, the proposed protocols, designed with a Quantum approach, can be effectively deployed on Amazon's AWS Braket Cloud computing platform.

   AWS Braket, a comprehensive quantum computing service by Amazon, offers a robust environment for implementing quantum-based security protocols. Notable features of AWS Braket include its ability to access a range of quantum computing hardware from different technology providers and integration with traditional cloud services. By leveraging AWS Braket, users can harness the power of quantum computing while benefitting from the secure and scalable infrastructure offered by Amazon Web Services.

3. **Quantum state Tomography:**
   The efficiency of Quantum-based schemes can be achieved through quantum state tomography This process involves the comprehensive characterization and analysis of quantum states to evaluate how well the Quantum states, integral to the authentication protocols, are prepared and maintained. Quantum state tomography plays a pivotal role in this evaluation by providing detailed insights into the quantum

states' characteristics, including their purity, coherence, and fidelity. This thorough examination ensures that the quantum states used in the authentication protocols align with the intended specifications. Furthermore, quantum state tomography's benefits extend beyond mere verification. By employing this technique, researchers and practitioners can better understand quantum states' behaviour, identify potential sources of error, and fine-tune the protocols for optimal performance.

4. **ProVerif and Scyther:**
   In IoT security and mutual authentication protocols, it is crucial to subject the proposed protocols to thorough testing and analysis. Experimentations of the proposed protocols can be simulated using ProVerif and Scyther tools and the AVISPA tool.

   ProVerif and Scyther, like AVISPA, play instrumental roles in evaluating the proposed security protocols. ProVerif, a formal verification tool, ensures the security objectives of the mutual authentication protocol are met. Similarly, Scyther formally analyses security protocols, providing insights into potential security flaws and vulnerabilities.

   Incorporating ProVerif and Scyther alongside the AVISPA tool in the simulation process offers a comprehensive and multi-faceted approach to protocol evaluation. This enables researchers and practitioners to scrutinize the protocols under diverse conditions, identify and rectify potential weaknesses, and validate the robustness of the mutual authentication mechanism within the IoT context. By conducting simulations across these tools, a more thorough understanding of the security properties of the protocols is achieved, ensuring a resilient foundation for IoT security implementations.

5. **Quantum Computers:**
   By exploring the real-world implementation of these protocols in Quantum Computing, researchers can understand the mutual authentication mechanism's practicality and adaptability within the evolving Quantum technologies landscape. This holistic evaluation is essential for developing robust and future-proof security solutions for IoT communication frameworks.

6. **Integration with Existing Healthcare Systems:**
   Future work could incorporate the proposed QSMAH protocol with established healthcare systems and IoT devices in real-world healthcare environments. This integration process must be carefully planned and executed to ensure compatibility and interoperability with different devices and systems.

Appendix A

List of Publications

International Journals

1. D. Chawla and P. S. Mehra, “A roadmap from classical cryptography to post-quantum resistant cryptography for 5G-enabled IoT: Challenges, opportunities and solutions,” Internet of Things, Elsevier, vol. 24, p. 100950, Dec. 2023.
   doi: https://doi.org/10.1016/j.iot.2023.100950 (SCIE- 5.9)

2. D. Chawla and P. S. Mehra, “QAKA: A Novel Quantum Authentication and Key Agreement (QAKA) protocol using Quantum Entanglement for Secure Communication among IoT Devices”, Transactions on Emerging Telecommunications Technologies, Wiley, vol.35, no.3, Jan 2024. doi: https://doi.org/10.1002/ett.4957 (SCIE-3.6)

3. D. Chawla and P. S. Mehra, “QSMAH: A novel quantum-based secure cryptosystem using mutual authentication for healthcare in the internet of things,” Internet of Things, Elsevier, vol. 24, p. 100949, Dec. 2023.
   doi: https://doi.org/10.1016/j.iot.2023.100949 (SCIE- 5.9)

4. QSSHA: Quantum Secured Smart Home Authentication Using Quantum Key Distribution and Maximally-Entangled States in IoT[Communicated].

5. A Survey on Quantum Cryptography Techniques for Secure Internet of Things Communication: Applications, Challenges and Roadmap[Communicated].

International Conferences

1. D. Chawla and P. S. Mehra, “A Survey on Quantum Computing for Internet of Things Security,” Procedia Computer Science, Elsevier, vol. 218, pp. 2191–2200, Jan. 2023, doi: https://doi.org/10.1016/j.procs.2023.01.195.

2. D. Chawla and P. S. Mehra, “Performance analysis of the Quantum schemes in the Resource-constrained IoT Network”, 4th International Conference on smart systems: Innovations in Computing, Springer, Oct 2023.[Article in Press]

Patent

1. D. Chawla and P. S. Mehra "Quantum cryptography based authentication system and method for secure transmission of healthcare data through GHZ states" Published(2023), Application Number: 202311064981, Indian Patent Office.

2. Secure Quantum Cryptography System and Method for Safe Communication and Storage of IoT-Based Data[Communicated].

Book Chapter

1. D. Chawla and P. S. Mehra, "Lightweight Cryptography Algorithms, Authorization and Authentication Techniques in IoT". Network Optimization in Intelligent IoT Applications– Principles and Challenges, CRC Press, Taylor and Francis.[Under publication]

References

[1] S. K. Routray, M. K. Jha, L. Sharma, R. Nyamangoudar, A. Javali, and S. Sarkar, "Quantum cryptography for iot: Aperspective," in *2017 International Conference on IoT and Application (ICIOT)*, pp. 1–4, IEEE, 2017.

[2] S. Challa, A. K. Das, V. Odelu, N. Kumar, S. Kumari, M. K. Khan, and A. V. Vasilakos, "An efficient ecc-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks," *Computers & Electrical Engineering*, vol. 69, pp. 534–554, 2018.

[3] F. Al-Turjman, H. Zahmatkesh, and R. Shahroze, "An overview of security and privacy in smart cities' iot communications," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 3, p. e3677, 2022.

[4] M. Al-Zubaidie, Z. Zhang, J. Zhang, *et al.*, "Ramhu: A new robust lightweight scheme for mutual users authentication in healthcare applications," *Security and Communication Networks*, vol. 2019, 2019.

[5] G. Yang, Q. Huang, D. S. Wong, and X. Deng, "Universal authentication protocols for anonymous wireless communications," *IEEE Transactions on Wireless Communications*, vol. 9, no. 1, pp. 168–174, 2010.

[6] M. S. Rahman and M. Hossam-E-Haider, "Quantum iot: A quantum approach in iot security maintenance," in *2019 International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST)*, pp. 269–272, IEEE, 2019.

[7] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on iot security: application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019.

[8] L. Chettri and R. Bera, "A comprehensive survey on internet of things (iot) toward 5g wireless systems," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 16–32, 2019.

[9] S. Li, L. Da Xu, and S. Zhao, "5g internet of things: A survey," *Journal of Industrial Information Integration*, vol. 10, pp. 1–9, 2018.

[10] H. Nagdewani and P. S. Mehra, "A complete internet of things based home security system," in *2022 Second International Conference on Computer Science, Engineering and Applications (ICCSEA)*, pp. 1–5, IEEE, 2022.

[11] O. Althobaiti, M. Al-Rodhaan, and A. Al-Dhelaan, "An efficient biometric authentication protocol for wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 9, no. 5, p. 407971, 2013.

[12] L. Wei, R. Q. Hu, Y. Qian, and G. Wu, "Key elements to enable millimeter wave communications for 5g wireless systems," *IEEE Wireless Communications*, vol. 21, no. 6, pp. 136–143, 2014.

[13] A. A. Zaidi, R. Baldemair, H. Tullberg, H. Bjorkegren, L. Sundstrom, J. Medbo, C. Kilinc, and I. Da Silva, "Waveform and numerology to support 5g services and requirements," *IEEE Communications Magazine*, vol. 54, no. 11, pp. 90–98, 2016.

[14] R. Chaudhary, N. Kumar, and S. Zeadally, "Network service chaining in fog and cloud computing for the 5g environment: Data management and security challenges," *IEEE Communications Magazine*, vol. 55, no. 11, pp. 114–122, 2017.

[15] Y. Niu, Y. Li, D. Jin, L. Su, and A. V. Vasilakos, "A survey of millimeter wave communications (mmwave) for 5g: opportunities and challenges," *Wireless networks*, vol. 21, pp. 2657–2676, 2015.

[16] S. Sharma, S. Satapathy, S. Singh, A. K. Sahu, M. S. Obaidat, S. Saxena, and D. Puthal, "Secure authentication protocol for 5g enabled iot network," in *2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC)*, pp. 621–626, IEEE, 2018.

[17] K. Shafique, B. A. Khawaja, F. Sabir, S. Qazi, and M. Mustaqim, "Internet of things (iot) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5g-iot scenarios," *Ieee Access*, vol. 8, pp. 23022–23040, 2020.

[18] M. Irfan, H. Jawad, B. B. Felix, S. F. Abbasi, A. Nawaz, S. Akbarzadeh, M. Awais, L. Chen, T. Westerlund, and W. Chen, "Non-wearable iot-based smart ambient behavior observation system," *IEEE Sensors Journal*, vol. 21, no. 18, pp. 20857–20869, 2021.

[19] I.-P. Chang, T.-F. Lee, T.-H. Lin, and C.-M. Liu, "Enhanced two-factor authentication and key agreement using dynamic identities in wireless sensor networks," *Sensors*, vol. 15, no. 12, pp. 29841–29854, 2015.

[20] A. C. Jose, R. Malekian, and B. B. Letswamotse, "Improving smart home security; integrating behaviour prediction into smart home," *International Journal of Sensor Networks*, vol. 28, no. 4, pp. 253–269, 2018.

[21] A. Braeken, P. Porambage, M. Stojmenovic, and L. Lambrinos, "edaaas: Efficient distributed anonymous authentication and access in smart homes," *International Journal of Distributed Sensor Networks*, vol. 12, no. 12, p. 1550147716682037, 2016.

[22] S. Yu, N. Jho, and Y. Park, "Lightweight three-factor-based privacy-preserving authentication scheme for iot-enabled smart homes," *IEEE Access*, vol. 9, pp. 126186–126197, 2021.

[23] S. Kailasam, S. D. M. Achanta, P. Rama Koteswara Rao, R. Vatambeti, and S. Kayam, "An iot-based agriculture maintenance using pervasive computing with machine learning technique," *International Journal of Intelligent Computing and Cybernetics*, vol. 15, no. 2, pp. 184–197, 2022.

[24] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, “Blockchain for iot security and privacy: The case study of a smart home,” in *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)*, pp. 618–623, IEEE, 2017.

[25] M. Gupta, M. Abdelsalam, S. Khorsandroo, and S. Mittal, “Security and privacy in smart farming: Challenges and opportunities,” *IEEE Access*, vol. 8, pp. 34564–34584, 2020.

[26] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, L. Shu, *et al.*, “Authentication protocols for internet of things: a comprehensive survey,” *Security and Communication Networks*, vol. 2017, 2017.

[27] M. A. Ferrag, L. Maglaras, and A. Derhab, “Authentication and authorization for mobile iot devices using biofeatures: Recent advances and future trends,” *Security and Communication Networks*, vol. 2019, 2019.

[28] L. Guo, C. Zhang, J. Sun, and Y. Fang, “A privacy-preserving attribute-based authentication system for mobile health networks,” *IEEE Transactions on Mobile Computing*, vol. 13, no. 9, pp. 1927–1941, 2013.

[29] A. Sampath Dakshina Murthy, T. Karthikeyan, and R. Vinoth Kanna, “Gait-based person fall prediction using deep learning approach,” *Soft Computing*, pp. 1–9, 2021.

[30] P. S. Mehra, Y. B. Mehra, A. Dagur, A. K. Dwivedi, M. Doja, and A. Jamshed, “Covid-19 suspected person detection and identification using thermal imaging-based closed circuit television camera and tracking using drone in internet of things,” *International Journal of Computer Applications in Technology*, vol. 66, no. 3-4, pp. 340–349, 2021.

[31] W. AL-mawee *et al.*, “Privacy and security issues in iot healthcare applications for the disabled users a survey,” 2012.

[32] S. Butt, J. Diaz-Martinez, T. Jamal, A. Ali, E. De-La-Hoz-Franco, and M. Shoaib, “Iot smart health security threats. proceedings-2019 19th international conference on computational science and its applications, iccsa 2019,(pp. 26–31),” *IEEE*, vol. 10, pp. 2019–000, 2019.

[33] I. Yusof and A.-S. K. Pathan, “Preventing persistent cross-site scripting (xss) attack by applying pattern filtering approach,” in *The 5th International Conference on Information and Communication Technology for The Muslim World (ICT4M)*, pp. 1–6, IEEE, 2014.

[34] S. Rathore, P. K. Sharma, and J. H. Park, “Xssclassifier: an efficient xss attack detection approach based on machine learning classifier on snss,” *Journal of Information Processing Systems*, vol. 13, no. 4, pp. 1014–1028, 2017.

[35] R. M. Thiyab, M. Ali, F. Basil, *et al.*, “The impact of sql injection attacks on the security of databases,” in *Proceedings of the 6th International Conference of Computing & Informatics*, pp. 323–331, School of Computing, 2017.

[36] L. Ntagwabira and S. L. Kang, "Use of query tokenization to detect and prevent sql injection attacks," in *2010 3rd International conference on computer science and information technology*, vol. 2, pp. 438–440, IEEE, 2010.

[37] R. Latif, H. Abbas, S. Latif, and A. Masood, "Distributed denial of service attack source detection using efficient traceback technique (ett) in cloud-assisted healthcare environment," *Journal of Medical Systems*, vol. 40, pp. 1–13, 2016.

[38] C.-M. Yu, Y.-T. Tsou, C.-S. Lu, and S.-Y. Kuo, "Constrained function-based message authentication for sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 2, pp. 407–425, 2011.

[39] I. Mistry, S. Tanwar, S. Tyagi, and N. Kumar, "Blockchain for 5g-enabled iot for industrial automation: A systematic review, solutions, and challenges," *Mechanical systems and signal processing*, vol. 135, p. 106382, 2020.

[40] K. Tsiknas, D. Taketzis, K. Demertzis, and C. Skianis, "Cyber threats to industrial iot: a survey on attacks and countermeasures," *IoT*, vol. 2, no. 1, pp. 163–186, 2021.

[41] M. Chandrasekaran, R. Chinchani, and S. Upadhyaya, "Phoney: Mimicking user response to detect phishing attacks," in *2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM'06)*, pp. 5–pp, IEEE, 2006.

[42] K. Demertzis, P. Kikiras, N. Tziritas, S. L. Sanchez, and L. Iliadis, "The next generation cognitive security operations center: network flow forensics using cybersecurity intelligence," *Big data and cognitive computing*, vol. 2, no. 4, p. 35, 2018.

[43] E. Stalmans and B. Irwin, "A framework for dns based detection and mitigation of malware infections on a network," in *2011 Information Security for South Africa*, pp. 1–8, IEEE, 2011.

[44] M. Al-Hawawreh, F. Den Hartog, and E. Sitnikova, "Targeted ransomware: A new cyber threat to edge system of brownfield industrial internet of things," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 7137–7151, 2019.

[45] O. M. Alhawi, J. Baldwin, and A. Dehghantanha, "Leveraging machine learning techniques for windows ransomware network traffic detection," *Cyber threat intelligence*, pp. 93–106, 2018.

[46] A. O. Almashhadani, M. Kaiiali, S. Sezer, and P. O'Kane, "A multi-classifier network-based crypto ransomware detection system: A case study of locky ransomware," *IEEE access*, vol. 7, pp. 47053–47067, 2019.

[47] R. Muraleedharan and L. A. Osadciw, "Cross layer denial of service attacks in wireless sensor network using swarm intelligence," in *2006 40th Annual Conference on Information Sciences and Systems*, pp. 1653–1658, IEEE, 2006.

[48] M. Jebalia, A. B. Letaifa, M. Hamdi, and S. Tabbane, "A revocation game model for secure cloud storage," in *2014 International Conference on High Performance Computing & Simulation (HPCS)*, pp. 1016–1017, IEEE, 2014.

[49] M. Usman, S. Raponi, M. Qaraqe, and G. Oligeri, “Kafhca: Key-establishment via frequency hopping collisions,” in *ICC 2021-IEEE International Conference on Communications*, pp. 1–6, IEEE, 2021.

[50] P. Radanliev, D. De Roure, K. Page, J. R. Nurse, R. Mantilla Montalvo, O. Santos, L. Maddox, and P. Burnap, “Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains,” *Cybersecurity*, vol. 3, no. 1, pp. 1–21, 2020.

[51] S. Raza, L. Wallgren, and T. Voigt, “Svelte: Real-time intrusion detection in the internet of things,” *Ad hoc networks*, vol. 11, no. 8, pp. 2661–2674, 2013.

[52] J. Cui, L. S. Liew, G. Sabaliauskaite, and F. Zhou, “A review on safety failures, security attacks, and available countermeasures for autonomous vehicles,” *Ad Hoc Networks*, vol. 90, p. 101823, 2019.

[53] Y. Ming and X. Shen, “Pcpa: A practical certificateless conditional privacy preserving authentication scheme for vehicular ad hoc networks,” *Sensors*, vol. 18, no. 5, p. 1573, 2018.

[54] Y. Hao, Y. Cheng, C. Zhou, and W. Song, “A distributed key management framework with cooperative message authentication in vanets,” *IEEE Journal on selected areas in communications*, vol. 29, no. 3, pp. 616–629, 2011.

[55] O. S. Althobaiti and M. Dohler, “Cybersecurity challenges associated with the internet of things in a post-quantum world,” *IEEE Access*, vol. 8, pp. 157356–157381, 2020.

[56] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” *arXiv preprint arXiv:2003.06557*, 2020.

[57] P. K. Panda and S. Chattopadhyay, “A secure mutual authentication protocol for iot environment,” *Journal of Reliable Intelligent Environments*, vol. 6, pp. 79–94, 2020.

[58] M. S. Sharbaf, “Quantum cryptography: a new generation of information technology security system,” in *2009 Sixth International Conference on Information Technology: New Generations*, pp. 1644–1648, IEEE, 2009.

[59] A. Lohachab *et al.*, “Using quantum key distribution and ecc for secure inter-device authentication and communication in iot infrastructure,” in *Proceedings of 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT)*, pp. 26–27, 2018.

[60] M. S. Sharbaf, “Quantum cryptography: An emerging technology in network security,” in *2011 IEEE International Conference on Technologies for Homeland Security (HST)*, pp. 13–19, IEEE, 2011.

[61] S. Krithika and T. Kesavmurthy, “Securing iot network through quantum key distribution,” *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, vol. 8, no. 6S4, pp. 2278–3075, 2019.

[62] V. K. Ralegankar, J. Bagul, B. Thakkar, R. Gupta, S. Tanwar, G. Sharma, and I. E. Davidson, "Quantum cryptography-as-a-service for secure uav communication: applications, challenges, and case study," *IEEE Access*, vol. 10, pp. 1475–1492, 2021.

[63] E. Rodríguez, J. Arqués, R. Rodríguez, M. Nuñez, M. Medina, T. Talarico, I. Casas, T. Chung, W. Dobrogosz, L. Axelsson, *et al.*, "We are intechopen, the world's leading publisher of open access books built by scientists, for scientists top 1%," *Intech*, vol. 32, no. tourism, pp. 137–144, 1989.

[64] V. Hassija, V. Chamola, V. Saxena, V. Chanana, P. Parashari, S. Mumtaz, and M. Guizani, "Present landscape of quantum computing," *IET Quantum Communication*, vol. 1, no. 2, pp. 42–48, 2020.

[65] V. Teja, P. Banerjee, N. Sharma, and R. Mittal, "Quantum cryptography: state-of-art, challenges and future perspectives," in *2007 7th IEEE conference on nanotechnology (IEEE NANO)*, pp. 1296–1301, IEEE, 2007.

[66] A. Lamas-Linares and C. Kurtsiefer, "Breaking a quantum key distribution system through a timing side channel," *Optics express*, vol. 15, no. 15, pp. 9388–9393, 2007.

[67] L. Xu and M. Wang, "A qds scheme based on superdense teleportation," *Quantum Information Processing*, vol. 21, no. 6, p. 220, 2022.

[68] T. Zhou, J. Shen, X. Li, C. Wang, and J. Shen, "Quantum cryptography for the future internet and the security analysis," *Security and Communication Networks*, vol. 2018, pp. 1–7, 2018.

[69] M. A. Ghonaimy, "An overview of quantum information systems," in *2013 8th International Conference on Computer Engineering & Systems (ICCES)*, pp. xx–xxxii, IEEE, 2013.

[70] A. Adeel, M. Gogate, S. Farooq, C. Ieracitano, K. Dashtipour, H. Larijani, and A. Hussain, "A survey on the role of wireless sensor networks and iot in disaster management," *Geological disaster monitoring based on sensor networks*, pp. 57–66, 2019.

[71] W. H. Wong, "Timing attacks on rsa: revealing your secrets through the fourth dimension," *XRDS: Crossroads, The ACM Magazine for Students*, vol. 11, no. 3, pp. 5–5, 2005.

[72] C. J. Mitchell, "The impact of quantum computing on real-world security: A 5g case study," *Computers & Security*, vol. 93, p. 101825, 2020.

[73] C. Cheng, R. Lu, A. Petzoldt, and T. Takagi, "Securing the internet of things in a quantum world," *IEEE Communications Magazine*, vol. 55, no. 2, pp. 116–120, 2017.

[74] A. B. Dorothy and S. B. R. Kumar, "An approach for iot security using quantum key distribution,"

[75] K. Dong, Y. Cao, Q. Yang, S. Zhang, H. Xing, and Q. Ren, "Role of hydrogen bonds in ionic-liquid-mediated extraction of natural bioactive homologues," *Industrial & engineering chemistry research*, vol. 51, no. 14, pp. 5299–5308, 2012.

[76] A. A. Zaidi, R. Baldemair, V. Molés-Cases, N. He, K. Werner, and A. Cedergren, "Ofdm numerology design for 5g new radio to support iot, embb, and mbsfn," *IEEE Communications Standards Magazine*, vol. 2, no. 2, pp. 78–83, 2018.

[77] D. Chawla and P. S. Mehra, "A survey on quantum computing for internet of things security," *Procedia Computer Science*, vol. 218, pp. 2191–2200, 2023.

[78] V. Kalaivani *et al.*, "Enhanced bb84 quantum cryptography protocol for secure communication in wireless body sensor networks for medical applications," *Personal and Ubiquitous Computing*, p. 1, 2021.

[79] L. Malina, L. Popelova, P. Dzurenda, J. Hajny, and Z. Martinasek, "On feasibility of post-quantum cryptography on small devices," *IFAC-PapersOnLine*, vol. 51, no. 6, pp. 462–467, 2018.

[80] S. Hassanpour and M. Houshmand, "Bidirectional teleportation of a pure epr state by using ghz states," *Quantum Information Processing*, vol. 15, no. 2, pp. 905–912, 2016.

[81] Y. Xu, C. Wang, X. Wang, and H. Zhu, "Scalable multiple ghz states equations and its applications in efficient quantum key agreement," *Quantum Information Processing*, vol. 21, no. 3, p. 91, 2022.

[82] A. K. Dwivedi, A. K. Sharma, and P. S. Mehra, "Energy efficient sensor node deployment scheme for two stage routing protocol of wireless sensor networks assisted iot," *ECTI Transactions on Electrical Engineering, Electronics, and Communications*, vol. 18, no. 2, pp. 158–169, 2020.

[83] S. S. Gill, A. Kumar, H. Singh, M. Singh, K. Kaur, M. Usman, and R. Buyya, "Quantum computing: A taxonomy, systematic review and future directions," *Software: Practice and Experience*, vol. 52, no. 1, pp. 66–114, 2022.

[84] P. Gupta, P. Raj, S. Tiwari, P. Kumari, and P. S. Mehra, "Energy efficient diagonal based clustering protocol in wireless sensor network," in *Proceedings of the International Conference on Innovative Computing & Communications (ICICC)*, 2020.

[85] S.-T. Cheng, C.-Y. Wang, and M.-H. Tao, "Quantum communication for wireless wide-area networks," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 7, pp. 1424–1432, 2005.

[86] Z. A. Abdulkader *et al.*, "A secure iot system using quantum cryptography with block cipher," *Journal of Applied Science and Engineering*, vol. 24, no. 5, pp. 771–776, 2021.

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

[88] R. Amin and G. Biswas, "A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks," *Ad Hoc Networks*, vol. 36, pp. 58–80, 2016.

[89] D. Sey, “A survey on authentication methods for the internet of things,” *PeerJ Preprints*, vol. 6, p. e26474v2, 2018.

[90] R. Melki, H. N. Noura, and A. Chehab, “Lightweight multi-factor mutual authentication protocol for iot devices,” *International Journal of Information Security*, vol. 19, pp. 679–694, 2020.

[91] D. Singh, B. Kumar, S. Singh, and S. Chand, “Evaluating authentication schemes for real-time data in wireless sensor network,” *Wireless Personal Communications*, vol. 114, pp. 629–655, 2020.

[92] R. Arul, G. Raja, A. O. Almagrabi, M. S. Alkatheiri, S. H. Chauhdary, and A. K. Bashir, “A quantum-safe key hierarchy and dynamic security association for lte/sae in 5g scenario,” *IEEE Transactions on Industrial Informatics*, vol. 16, no. 1, pp. 681–690, 2019.

[93] M. Wazid, A. K. Das, S. Shetty, P. Gope, and J. J. Rodrigues, “Security in 5g-enabled internet of things communication: issues, challenges, and future research roadmap,” *IEEE Access*, vol. 9, pp. 4466–4489, 2020.

[94] J. Cao, P. Yu, X. Xiang, M. Ma, and H. Li, “Anti-quantum fast authentication and data transmission scheme for massive devices in 5g nb-iot system,” *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 9794–9805, 2019.

[95] J. Ni, X. Lin, and X. S. Shen, “Efficient and secure service-oriented authentication supporting network slicing for 5g-enabled iot,” *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 3, pp. 644–657, 2018.

[96] L. SPALAZZI and S. TACCONI, “Classification of attacks on cryptographic protocols,” *Handbook of Electronic Security and Digital Forensics, World Scientific Publishing, Singapore*, pp. 47–82, 2010.

[97] D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, and V. Stettler, “A formal analysis of 5g authentication,” in *Proceedings of the 2018 ACM SIGSAC conference on computer and communications security*, pp. 1383–1396, 2018.

[98] S. Gong, A. El Azzaoui, J. Cha, and J. H. Park, “Secure secondary authentication framework for efficient mutual authentication on a 5g data network,” *Applied Sciences*, vol. 10, no. 2, p. 727, 2020.

[99] R. Watro, D. Kong, S.-f. Cuti, C. Gardiner, C. Lynn, and P. Kruus, “Tinypk: securing sensor networks with public key technology,” in *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*, pp. 59–64, 2004.

[100] M. L. Das, “Two-factor user authentication in wireless sensor networks,” *IEEE transactions on wireless communications*, vol. 8, no. 3, pp. 1086–1090, 2009.

[101] A. Zhang, J. Chen, R. Q. Hu, and Y. Qian, “Seds: Secure data sharing strategy for d2d communication in lte-advanced networks,” *IEEE Transactions on Vehicular Technology*, vol. 65, no. 4, pp. 2659–2672, 2015.

[102] P. S. Mehra, M. N. Doja, and B. Alam, "Codeword authenticated key exchange (cake) light weight secure routing protocol for wsn," *International Journal of Communication Systems*, vol. 32, no. 3, p. e3879, 2019.

[103] S. Wang, J. Wang, and Z. Yu, "Privacy-preserving authentication in wireless iot: applications, approaches, and challenges," *IEEE Wireless Communications*, vol. 25, no. 6, pp. 60–67, 2018.

[104] S. F. Abbasi, J. Ahmad, J. S. Khan, M. A. Khan, and S. A. Sheikh, "Visual meaningful encryption scheme using intertwinning logistic map," in *Intelligent Computing: Proceedings of the 2018 Computing Conference, Volume 2*, pp. 764–773, Springer, 2019.

[105] G. Avoine, S. Canard, and L. Ferreira, "Iot-friendly ake: forward secrecy and session resumption meet symmetric-key cryptography," in *Computer Security–ESORICS 2019: 24th European Symposium on Research in Computer Security, Luxembourg, September 23–27, 2019, Proceedings, Part II 24*, pp. 463–483, Springer, 2019.

[106] M. Turkanović, B. Brumen, and M. Hölbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion," *Ad Hoc Networks*, vol. 20, pp. 96–112, 2014.

[107] Y. Lu, G. Xu, L. Li, and Y. Yang, "Anonymous three-factor authenticated key agreement for wireless sensor networks," *Wireless Networks*, vol. 25, pp. 1461–1475, 2019.

[108] M. S. Farash, M. Turkanović, S. Kumari, and M. Hölbl, "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the internet of things environment," *Ad Hoc Networks*, vol. 36, pp. 152–176, 2016.

[109] P. Gope, R. Amin, S. H. Islam, N. Kumar, and V. K. Bhalla, "Lightweight and privacy-preserving rfid authentication scheme for distributed iot infrastructure with secure localization services for smart city environment," *Future Generation Computer Systems*, vol. 83, pp. 629–637, 2018.

[110] B. Di Ying, D. Makrakis, and H. T. Mouftah, "Anti-traffic analysis attack for location privacy in wsns," *EURASIP Journal on Wireless Communications and Networking*, vol. 2014, no. 1, pp. 1–15, 2014.

[111] A. A. Abd EL-Latif, B. Abd-El-Atty, S. E. Venegas-Andraca, and W. Mazurczyk, "Efficient quantum-based security protocols for information sharing and data protection in 5g networks," *Future Generation Computer Systems*, vol. 100, pp. 893–906, 2019.

[112] S. Amanlou, M. K. Hasan, and K. A. A. Bakar, "Lightweight and secure authentication scheme for iot network based on publish–subscribe fog computing model," *Computer Networks*, vol. 199, p. 108465, 2021.

[113] A. K. Das, P. Sharma, S. Chatterjee, and J. K. Sing, "A dynamic password-based user authentication scheme for hierarchical wireless sensor networks," *Journal of Network and Computer Applications*, vol. 35, no. 5, pp. 1646–1656, 2012.

[114] S. Kumari and H. Om, "Authentication protocol for wireless sensor networks applications like safety monitoring in coal mines," *Computer Networks*, vol. 104, pp. 137–154, 2016.

[115] Q. Jiang, J. Ma, F. Wei, Y. Tian, J. Shen, and Y. Yang, "An untraceable temporal-credential-based two-factor authentication scheme using ecc for wireless sensor networks," *Journal of Network and Computer Applications*, vol. 76, pp. 37–48, 2016.

[116] C.-C. Chang and H.-D. Le, "A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks," *IEEE Transactions on wireless communications*, vol. 15, no. 1, pp. 357–366, 2015.

[117] B. Vaidya, D. Makrakis, and H. T. Mouftah, "Improved two-factor user authentication in wireless sensor networks," in *2010 IEEE 6th international conference on wireless and mobile computing, networking and communications*, pp. 600–606, IEEE, 2010.

[118] M. K. Khan and S. Kumari, "An improved user authentication protocol for healthcare services via wireless medical sensor networks," *International Journal of Distributed Sensor Networks*, vol. 10, no. 4, p. 347169, 2014.

[119] B. D. Deebak, "Secure and efficient mutual adaptive user authentication scheme for heterogeneous wireless sensor networks using multimedia client–server systems," *Wireless Personal Communications*, vol. 87, pp. 1013–1035, 2016.

[120] D. Mishra, P. Vijayakumar, V. Sureshkumar, R. Amin, S. H. Islam, and P. Gope, "Efficient authentication protocol for secure multimedia communications in iot-enabled wireless sensor networks," *Multimedia Tools and Applications*, vol. 77, pp. 18295–18325, 2018.

[121] H. Li, F. Li, C. Song, and Y. Yan, "Towards smart card based mutual authentication schemes in cloud computing," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 9, no. 7, pp. 2719–2735, 2015.

[122] N. Park and N. Kang, "Mutual authentication scheme in secure internet of things technology for comfortable lifestyle," *Sensors*, vol. 16, no. 1, p. 20, 2015.

[123] A. I. Nurhadi and N. R. Syambas, "Quantum key distribution (qkd) protocols: A survey," in *2018 4th International Conference on Wireless and Telematics (ICWT)*, pp. 1–5, IEEE, 2018.

[124] P. Longa, "A note on post-quantum authenticated key exchange from supersingular isogenies," *Cryptology ePrint Archive*, 2018.

[125] L. Malina, P. Dzurenda, S. Ricci, J. Hajny, G. Srivastava, R. Matulevičius, A.-A. O. Affia, M. Laurent, N. H. Sultan, and Q. Tang, "Post-quantum era privacy protection for intelligent infrastructures," *IEEE Access*, vol. 9, pp. 36038–36077, 2021.

[126] A. Kumar and S. Garhwal, "State-of-the-art survey of quantum cryptography," *Archives of Computational Methods in Engineering*, vol. 28, pp. 3831–3868, 2021.

[127] K. Kadian, S. Garhwal, and A. Kumar, "Quantum walk and its application domains: A systematic review," *Computer Science Review*, vol. 41, p. 100419, 2021.

[128] R. Amiri, R. Stárek, D. Reichmuth, I. V. Puthoor, M. Mičuda, L. Mišta Jr, M. Dušek, P. Wallden, and E. Andersson, "Imperfect 1-out-of-2 quantum oblivious transfer: bounds, a protocol, and its experimental implementation," *PRX Quantum*, vol. 2, no. 1, p. 010335, 2021.

[129] G. C. Pereira, C. Puodzius, and P. S. Barreto, "Shorter hash-based signatures," *Journal of Systems and Software*, vol. 116, pp. 95–100, 2016.

[130] A. A. Abd El-Latif, B. Abd-El-Atty, S. E. Venegas-Andraca, H. Elwahsh, M. J. Piran, A. K. Bashir, O.-Y. Song, and W. Mazurczyk, "Providing end-to-end security using quantum walks in iot networks," *IEEE Access*, vol. 8, pp. 92687–92696, 2020.

[131] M. Niemiec, "Error correction in quantum cryptography based on artificial neural networks," *Quantum Information Processing*, vol. 18, no. 6, p. 174, 2019.

[132] D. J. Bernstein, *Introduction to post-quantum cryptography.* Springer, 2009.

[133] N. Göttert, T. Feller, M. Schneider, J. Buchmann, and S. Huss, "On the design of hardware building blocks for modern lattice-based encryption schemes," in *Cryptographic Hardware and Embedded Systems–CHES 2012: 14th International Workshop, Leuven, Belgium, September 9-12, 2012. Proceedings 14*, pp. 512–529, Springer, 2012.

[134] Z. Liu, K.-K. R. Choo, and J. Grossschadl, "Securing edge devices in the post-quantum internet of things using lattice-based cryptography," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 158–162, 2018.

[135] R. Niederhagen and M. Waidner, "Practical post-quantum cryptography," *Fraunhofer SIT*, 2017.

[136] A. Boorghany, S. B. Sarmadi, and R. Jalili, "On constrained implementation of lattice-based cryptographic primitives and schemes on smart cards," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 14, no. 3, pp. 1–25, 2015.

[137] R. Overbeck and N. Sendrier, "Code-based cryptography," *Post-quantum cryptography*, pp. 95–145, 2009.

[138] S. De Capitani di Vimercati, S. Foresti, G. Livraga, and P. Samarati, "Practical techniques building on encryption for protecting and managing data in the cloud," *The New Codebreakers: Essays Dedicated to David Kahn on the Occasion of His 85th Birthday*, pp. 205–239, 2016.

[139] S. Streit and F. De Santis, "Post-quantum key exchange on armv8-a: A new hope for neon made simple," *IEEE Transactions on Computers*, vol. 67, no. 11, pp. 1651–1662, 2017.

[140] U. Vazirani and T. Vidick, "Distribución de clave cuántica totalmente independiente del dispositivo," *Phys. Rev. Lett*, vol. 113, no. 140501, pp. 10–1103, 2014.

[141] J. Buchmann, E. Dahmen, and A. Hülsing, "Xmss-a practical forward secure signature scheme based on minimal security assumptions," in *Post-Quantum Cryptography: 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29–December 2, 2011. Proceedings 4*, pp. 117–129, Springer, 2011.

[142] J. Illiano, M. Caleffi, A. Manzalini, and A. S. Cacciapuoti, “Quantum internet protocol stack: A comprehensive survey,” *Computer Networks*, vol. 213, p. 109092, 2022.

[143] S. Rajiuddin, A. Baishya, B. K. Behera, and P. K. Panigrahi, “Experimental realization of quantum teleportation of an arbitrary two-qubit state using a four-qubit cluster state,” *Quantum Information Processing*, vol. 19, pp. 1–13, 2020.

[144] S. R. Moulick and P. K. Panigrahi, “Quantum cheques,” *Quantum Information Processing*, vol. 15, pp. 2475–2486, 2016.

[145] H.-C. Chen, C. Damarjati, E. Prasetyo, C.-L. Chou, T.-L. Kung, and C.-E. Weng, “Generating multi-issued session key by using semi quantum key distribution with time-constraint,” *IEEE Access*, vol. 10, pp. 20839–20851, 2022.

[146] S. Kumari, X. Li, F. Wu, A. K. Das, H. Arshad, and M. K. Khan, “A user friendly mutual authentication and key agreement scheme for wireless sensor networks using chaotic maps,” *Future Generation Computer Systems*, vol. 63, pp. 56–75, 2016.

[147] G. Sharma and S. Kalra, “A lightweight multi-factor secure smart card based remote user authentication scheme for cloud-iot applications,” *Journal of information security and applications*, vol. 42, pp. 95–106, 2018.

[148] M. K. Khan and K. Alghathbar, “Cryptanalysis and security improvements of ‘two-factor user authentication in wireless sensor networks’,” *Sensors*, vol. 10, no. 3, pp. 2450–2459, 2010.

[149] X. Li, J. Niu, S. Kumari, F. Wu, A. K. Sangaiah, and K.-K. R. Choo, “A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments,” *Journal of Network and Computer Applications*, vol. 103, pp. 194–204, 2018.

[150] B. K. Behera, A. Banerjee, and P. K. Panigrahi, “Experimental realization of quantum cheque using a five-qubit quantum computer,” *Quantum Information Processing*, vol. 16, pp. 1–12, 2017.

[151] K. S. Roy and H. K. Kalita, “A quantum safe user authentication protocol for the internet of things,” *International Journal of Next-Generation Computing*, vol. 10, no. 3, 2019.

[152] N. Nagy, M. Nagy, and S. G. Akl, “Quantum security in wireless sensor networks,” *Natural Computing*, vol. 9, pp. 819–830, 2010.

[153] A. Punia, M. Tiwari, and S. S. Verma, “The iot in security architecture, challenges, and solutions,” in *International Conference on Optical and Wireless Technologies*, pp. 405–416, Springer, 2021.

[154] S. Shukla, S. Thakur, S. Hussain, J. G. Breslin, and S. M. Jameel, “Identification and authentication in healthcare internet-of-things using integrated fog computing based blockchain model,” *Internet of Things*, vol. 15, p. 100422, 2021.

[155] C. Shao, Y. Li, and H. Li, “Quantum algorithm design: techniques and applications,” *Journal of Systems Science and Complexity*, vol. 32, pp. 375–452, 2019.

[156] B. Langenberg, H. Pham, and R. Steinwandt, "Reducing the cost of implementing the advanced encryption standard as a quantum circuit," *IEEE Transactions on Quantum Engineering*, vol. 1, pp. 1–12, 2020.

[157] M. Campagna and E. Crockett, "Hybrid post-quantum key encapsulation methods (pq kem) for transport layer security 1.2 (tls)," *Internet Engineering Task Force, Internet-Draft draft-campagna-tls-bike-sike-hybrid*, vol. 1, 2019.

[158] N. Chikouche, P.-L. Cayrel, E. H. M. Mboup, and B. O. Boidje, "A privacy-preserving code-based authentication protocol for internet of things," *The Journal of Supercomputing*, vol. 75, pp. 8231–8261, 2019.

[159] M. Elhoseny, G. Ramírez-González, O. M. Abu-Elnasr, S. A. Shawkat, N. Arunkumar, and A. Farouk, "Secure medical data transmission model for iot-based healthcare systems," *Ieee Access*, vol. 6, pp. 20596–20608, 2018.

[160] T.-J. Xu, Y. Chen, M.-J. Geng, and T.-Y. Ye, "Single-state multi-party semiquantum key agreement protocol based on multi-particle ghz entangled states," *Quantum Information Processing*, vol. 21, no. 7, p. 266, 2022.

[161] A. N. Bahache, N. Chikouche, and F. Mezrag, "Authentication schemes for healthcare applications using wireless medical sensor networks: A survey," *SN Computer Science*, vol. 3, no. 5, p. 382, 2022.

[162] R. Ur Rasool, H. F. Ahmad, W. Rafique, A. Qayyum, J. Qadir, and Z. Anwar, "Quantum computing for healthcare: A review," *Future Internet*, vol. 15, no. 3, p. 94, 2023.

[163] N. Alsaeed and F. Nadeem, "Authentication in the internet of medical things: Taxonomy, review, and open issues," *Applied Sciences*, vol. 12, no. 15, p. 7487, 2022.

[164] R. Amin, S. H. Islam, G. Biswas, M. K. Khan, and N. Kumar, "A robust and anonymous patient monitoring system using wireless medical sensor networks," *Future Generation Computer Systems*, vol. 80, pp. 483–495, 2018.

[165] G. Sharma and S. Kalra, "Identity based secure authentication scheme based on quantum key distribution for cloud computing," *Peer-to-Peer Networking and applications*, vol. 11, pp. 220–234, 2018.

[166] N. Li, D. Liu, and S. Nepal, "Lightweight mutual authentication for iot and its applications," *IEEE Transactions on Sustainable Computing*, vol. 2, no. 4, pp. 359–370, 2017.

[167] A. Dash, S. Rout, B. K. Behera, and P. K. Panigrahi, "Quantum locker using a novel verification algorithm and its experimental realization in ibm quantum computer," *arXiv preprint arXiv:1710.05196*, 2017.

[168] V. Kalaivani *et al.*, "Enhanced bb84 quantum cryptography protocol for secure communication in wireless body sensor networks for medical applications," *Personal and Ubiquitous Computing*, vol. 27, no. 3, p. 875, 2023.

[169] D. Chawla and P. S. Mehra, "Qsmah: A novel quantum-based secure cryptosystem using mutual authentication for healthcare in the internet of things," *Internet of Things*, vol. 24, p. 100949, 2023.

[170] P. S. Mehra, "Lbecr: load balanced, efficient clustering and routing protocol for sustainable internet of things in smart cities," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 8, pp. 10493–10515, 2023.

[171] A. Kumar Dwivedi, A. Sharma, Manju, S. Singh, and P. Mehra, "Scszb: Sensor congregate stable zonal-based routing protocol designed for optimal wsn," in *Advances in Smart Communication and Imaging Systems: Select Proceedings of MedCom 2020*, pp. 139–149, Springer, 2021.

Author Biography

Diksha Chawla received her B.Tech. in Information Technology from the Hindu College of Engineering, Haryana, India and her M.TECH in Information Technology from the Center for Development of Advanced Computing (CDAC), Noida, India. She is pursuing her Ph.D in the Department of Computer Science and Engineering at Delhi Technological University, New Delhi, India. She has more than 12 years of teaching experience. Her research areas include the Internet of Things, Quantum Information and Computing, Wireless Sensor Networks, Blockchain and Image Processing.